

A Study of Computer Forensics from a Cross-Cultural Perspective: Australia and Taiwan

By

Yi-Chi Lin

Thesis submitted to

The University of South Australia

For the degree of Doctor of Philosophy

March 2008

Primary Supervisor : Associate Professor Jill Slay

Associate Supervisor: Rodney Mckemmish

Accociate Supervisor: I-Long Lin

Abstract

The rise in the number and variety of digital devices has changed all facets of society, from the way we work and communicate to how our lives are recorded. Computers, notebooks, networks, mobile phones, digital cameras and embedded devices are all readily available and it is difficult to imagine a person that does not own at least some of these. However, with this rise in the use of electronics, comes its potential misuse. Electronic devices have transformed how existing crimes may occur, and also have allowed for several new forms of illegal activity. However, given the global nature of the Internet, such crimes may take place over multiple jurisdictions and countries.

Where the investigation into computer-based crime occurs between two or more countries, there is a need for the two teams to understand the legal and cultural differences between them. Whilst the legal differences are written, interpreted and can be made explicit, there is less knowledge on the cultural differences between two countries, working in an emerging scientific field.

Literature not only shows that the applications of science are affected by culture, but also demonstrates that computer forensics is a subject within the field of science. This research seeks to answer the question: *Does Culture have impacts on Applications of Computer Forensics?* In order to seek the answer of this problem, at least two countries with different cultural backgrounds and customs will be examined. Specifically, this work will discuss Australia and Taiwan, as these countries are examples of distinctive cultural variations found in the Asia Pacific.

Culture is difficult to directly measure, and this work utilises the Delphi survey technique and case study interviews of computer forensic professionals and experts in the field in both Australia and Taiwan as its primary source of data collection. Analysis of this data provides both a view of the field at large, provided by the Delphi survey results and more detailed knowledge from specific experts gathered from the interviews. Specifically, the Delphi survey has 40 questions in five dimensions (*Current Situation*, *Policy and Organization*, *Education*, *Law*, and *Personal Preference and Skill*), and the interview is comprised of 13 questions, each asking for more depth than the Delphi can provide.

The outcomes of this research directly compare the Australian and Taiwanese cultures as they apply to the field of computer forensics. As such, the most tangible outcome is a framework for Australian and Taiwanese law enforcement, forensic science community, and the court. The suggestions for cross-cultural, cross-border and collaborative digital forensic investigations can be provided based on the discoveries of this research. This thesis essentially helps the mutual understanding between Australian and Taiwanese computer forensic investigators. The understanding is able to improve the chances of success of future cooperation between Australia and Taiwan.

Acknowledgment

First of all, I would like to thank my parents, (Chun-Te Lin and Chun-Ling Lu), for their emotional and financial support and for allowing me the opportunity to study overseas in the PhD program in University of South Australia. I am particularly grateful to my wife, (Ching-Yi Lin), since she has supported my family in my place. With her help, I have been able to finish this thesis without any anxiety.

Secondly, I appreciate the assistance of my primary supervisor, Jill Slay. She is the person who has led me into this field, and has guided me when I have been confused. In addition, I have two associate supervisors, Rodney McKemmish and I-Long Lin. They have shared their valuable experience with me and have always pointed out the correct direction when I have had any doubt. My supervision group has helped me to understand that there is knowledge beyond my understanding and I should respect things or concepts that I am not familiar with.

Thirdly, I have two Australian friends, who have also studied in the PhD program in the University of South Australia, and these are Ben Turnbull and Tom Wilsdon. Ben always helps me to correct my English grammar, and provide useful suggestions for my research as well. I have learnt many things from him. Tom is a typical Australian and has not only shown me the Australian way of life, but has also helped me to further understand Australian culture. They have enabled me to realize the meaning of friendship.

Lastly, I would like to show my appreciation to the Australian and Taiwanese computer forensic experts, who provided their constructive opinions for both the Delphi surveys and the case study interviews. Due to their help, this thesis has been able to produce useful suggestions for cross-cultural cooperation between Australia and Taiwan. I am indebted to them and would not have been able to complete this research without their help.

Abstract *2*
Acknowledgment *4*
List of Figures *11*
List of Tables *12*
Acronyms and Abbreviations *13*
1 Introduction *15*
1.1 Introduction of this Thesis **16**
1.2 Aim of this Research **18**
1.3 Research Motivation **18**
1.4 Research Question **20**
1.5 Research Limitations **20**
1.6 Summary of this Chapter **22**
2 Literature Review *23*
2.1 Overview of this Chapter **24**
2.2 Computer Forensics **25**
2.2.1 Overview of this Section 25
2.2.2 What is Computer Forensics? 26
2.2.2.1 Definition of Computer Forensics 26
2.2.2.2 Purpose of Computer Forensics 28
2.2.2.3 Introduction of Digital Evidence 31
2.2.2.4 Definition of Digital Evidence 33
2.2.2.5 Traits of Digital Evidence 34
2.2.2.5.1 Metadata 34
2.2.2.5.2 Time Stamp 35
2.2.2.5.3 Integrity 37
2.2.2.5.4 Authentication 38
2.2.2.5.5 Reproducibility 38
2.2.2.5.6 Non-Interference 40
2.2.3 Procedures of Computer Forensics 41
2.2.3.1 Research-Based General Procedures of Computer Forensics 43
2.2.3.2 Practitioner-Based General Procedures of Computer Forensics 55
2.2.3.3 Standard Operating Procedure of Computer Forensics 68
2.2.4 Current Issues of Computer Forensics 70
2.2.4.1 Certification of Computer Forensics 70
2.2.4.2 Encryption in Computer Forensics 72
2.2.4.3 Electronic Discovery 74
2.2.5 Is Computer Forensics Science? 77
2.2.6 Summary of Section 2.2 78
2.3 Culture **78**
2.3.1 Overview of this Section 78
2.3.2 Definition of Culture 79
2.3.3 Culture and Science 80
2.3.4 Studies of Culture, Science, and Systems 83
2.3.4.1 Slay's Works 84
2.3.4.1.1 Culture and Conceptualisations of Nature 86
2.3.4.1.2 Culture and Science Education 88
2.3.4.1.3 Culture and Information System 88
2.3.4.2 Hofstede's Works 90
2.3.4.2.1 Dimensions of National Culture 90
2.3.4.2.2 Data Sources of Five Dimensions of National Culture 94
2.3.5 Summary of Section 2.3 97
2.4 Summary of this Chapter **97**

3 Methodology 99

3.1 Overview of this Chapter 100

3.2 Positivist and Interpretivist Research 101

3.3 Choice of Methods 103
3.3.1 Overview of this Section 103
3.3.2 Choices between Quantitative Research and Qualitative Research 103
3.3.3 Quantitative Research 105
3.3.4 Qualitative Research 106
3.3.5 Summary of Section 3.3 107

3.4 Quality of Qualitative Research 108
3.4.1 Overview of this Section 108
3.4.2 Validity of Quantitative Research (Positivist Research) 108
3.4.3 Reliability of Quantitative Research (Positivist Research) 110
3.4.4 Alternative Terms for Qualitative Research (Interpretivist Research) 111
3.4.4.1 Internal Validity and Credibility 112
3.4.4.2 External Validity and Transferability 113
3.4.4.3 Reliability and Dependability 114
3.4.5 Triangulation 115
3.4.5.1 Historical Data 116
3.4.5.2 Delphi Method 117
3.4.5.3 Case Study 118
3.4.6 Summary of Section 3.4 119

3.5 Delphi Survey Method 119
3.5.1 Overview of this Section 119
3.5.2 Purpose of Delphi Method 120
3.5.3 Characteristics of Delphi Method 121
3.5.4 Advantages of Delphi Method 122
3.5.5 Disadvantages of Delphi Method 123
3.5.6 Procedures of Delphi Method 124
3.5.7 Number of Panellists of Delphi Method 128
3.5.8 Limitations of Delphi Method 129
3.5.9 Quality of Delphi Method 131
3.5.9.1 Quality of Delphi Panellists 132
3.5.9.1.1 Quality of Australian Delphi Panellists 133
3.5.9.1.2 Quality of Taiwanese Delphi Panellists 133
3.5.9.2 Quality of Delphi Questionnaire 134
3.5.9.2.1 Current Situation Dimension 135
3.5.9.2.2 Policy and Organization Dimension 138
3.5.9.2.3 Education Dimension 139
3.5.9.2.4 Law Dimension 140
3.5.9.2.5 Personal Preference and Skill Dimension 140
3.5.10 Summary of Section 3.5 141

3.6 Case Study 142
3.6.1 Overview of this Section 142
3.6.2 Definition of Case Study 143
3.6.3 Design of Case Study 143
3.6.4 Data Sources of Case Study 144
3.6.5 Data Collection of Case Study 147
3.6.6 Quality of Case Study 148
3.6.6.1 Quality of Case Study Participants 149
3.6.6.1.1 Quality of Australian Case Study Participants 149
3.6.6.1.2 Quality of Taiwanese Case Study Participants 150
3.6.6.2 Quality of Case Study Questionnaire 150
3.6.6.2.1 Current Situation Dimension 150
3.6.6.2.2 Policy and Organization Dimension 151
3.6.6.2.3 Education Dimension 151
3.6.6.2.4 Law Dimension 152
3.6.6.2.5 Personal Preference and Skill Dimension 152
3.6.7 Summary of Section 3.6 153

3.7 Summary of this Chapter 153

4 Research Findings in Australia 155

4.1 Overview of this Chapter 156

4.2 Delphi Survey 156
4.2.1 Experts of the Delphi Survey 157
4.2.2 Findings of Delphi Survey 157
4.2.2.1 Current Situation Dimension 158
4.2.2.2 Policy and Organization Dimension 159
4.2.2.3 Education Dimension 160
4.2.2.4 Law Dimension 161
4.2.2.5 Personal Preferences and Skills Dimension 162
4.2.3 Interpretations of Delphi Results 162
4.2.3.1 Current Situation Dimension 163
4.2.3.2 Policy and Organization Dimension 173
4.2.3.3 Education Dimension 177
4.2.3.4 Law Dimension 181
4.2.3.5 Personal Preferences and Skills Dimension 184
4.2.3.6 Cross Questions 187
4.2.4 Summary of Section 4.2 189

4.3 Case Study 189
4.3.1 First Australian Case Study 190
4.3.1.1 Findings of the First Case Study 190
4.3.1.1.1 Current Situation Dimension 190
4.3.1.1.2 Policy and Organization Dimension 192
4.3.1.1.3 Education Dimension 192
4.3.1.1.4 Law Dimension 193
4.3.1.1.5 Personal Preference and Skill Dimension 194
4.3.1.2 Interpretations of the First Case Study Findings 195
4.3.1.2.1 Current Situation Dimension 195
4.3.1.2.2 Policy and Organization Dimension 197
4.3.1.2.3 Education Dimension 198
4.3.1.2.4 Law Dimension 200
4.3.1.2.5 Personal Preference and Skill Dimension 201
4.3.1.2.6 Cross Questions 202
4.3.2 Second Australian Case Study 203
4.3.2.1 Findings of the Second Case Study 204
4.3.2.1.1 Current Situation Dimension 204
4.3.2.1.2 Policy and Organization Dimension 205
4.3.2.1.3 Education Dimension 206
4.3.2.1.4 Law Dimension 207
4.3.2.1.5 Personal Preference and Skill Dimension 208
4.3.2.2 Interpretations of the Second Case Study Findings 208
4.3.2.2.1 Current Situation Dimension 208
4.3.2.2.2 Policy and Organization Dimension 210
4.3.2.2.3 Education Dimension 211
4.3.2.2.4 Law Dimension 213
4.3.2.2.5 Personal Preference and Skill Dimension 214
4.3.2.2.6 Cross Questions 215
4.3.3 Comparison of Australian Case Studies 215
4.3.4 Summary of Section 4.3 217

4.4 Triangulation of Findings in Australia 217
4.4.1 Triangulation of Research Methods 217
4.4.2 Corroboration for Delphi Survey and Case Study 219
4.4.3 Summary of Section 4.4 224

4.5 Summary of this Chapter 224

5 Research Findings in Taiwan 226

5.1 Overview of this Chapter 227

5.2 Delphi Survey....227
5.2.1 Experts of the Delphi Survey....228
5.2.2 Findings of Delphi Survey....228
5.2.2.1 Current Situation Dimension....229
5.2.2.2 Policy and Organization Dimension....230
5.2.2.3 Education Dimension....231
5.2.2.4 Law Dimension....232
5.2.2.5 Personal Preferences and Skills Dimension....233
5.2.3 Interpretations of Delphi Results....233
5.2.3.1 Current Situation Dimension....234
5.2.3.2 Policy and Organization Dimension....244
5.2.3.3 Education Dimension....248
5.2.3.4 Law Dimension....252
5.2.3.5 Personal Preferences and Skills Dimension....255
5.2.3.6 Cross Questions....258
5.2.4 Summary of Section 5.2....259

5.3 Case Study....260
5.3.1 First Taiwanese Case Study....260
5.3.1.1 Findings of the First Case Study....261
5.3.1.1.1 Current Situation Dimension....261
5.3.1.1.2 Policy and Organization Dimension....262
5.3.1.1.3 Education Dimension....263
5.3.1.1.4 Law Dimension....264
5.3.1.1.5 Personal Preference and Skill Dimension....265
5.3.1.2 Interpretations of the First Case Study Findings....266
5.3.1.2.1 Current Situation Dimension....266
5.3.1.2.2 Policy and Organization Dimension....268
5.3.1.2.3 Education Dimension....270
5.3.1.2.4 Law Dimension....272
5.3.1.2.5 Personal Preference and Skill Dimension....273
5.3.1.2.6 Cross Questions....274
5.3.2 Second Taiwanese Case Study....274
5.3.2.1 Findings of the Second Case Study....275
5.3.2.1.1 Current Situation Dimension....275
5.3.2.1.2 Policy and Organization Dimension....276
5.3.2.1.3 Education Dimension....277
5.3.2.1.4 Law Dimension....278
5.3.2.1.5 Personal Preference and Skill Dimension....279
5.3.2.2 Interpretations of the Second Case Study Findings....280
5.3.2.2.1 Current Situation Dimension....280
5.3.2.2.2 Policy and Organization Dimension....282
5.3.2.2.3 Education Dimension....283
5.3.2.2.4 Law Dimension....285
5.3.2.2.5 Personal Preference and Skill Dimension....286
5.3.2.2.6 Cross Questions....286
5.3.3 Comparison of Taiwanese Case Studies....287
5.3.4 Summary of Section 5.3....288

5.4 Triangulation and Corroboration of Research Results....289
5.4.1 Triangulation of Research Methods....289
5.4.2 Corroboration for Delphi Survey and Case Study....290
5.4.3 Summary of Section 5.4....295

5.5 Summary of this Chapter....295

6 Discussion on the Differences between Australian and Taiwanese Culture 297

6.1 Overview of this Chapter....298

6.2 Current Situation Dimension....298

6.3 Policy and Organization Dimension....303

6.4 Education Dimension....307

6.5 Law Dimension 311

6.6 Personal Preferences and Skills Dimension 313

6.7 Characteristics of Australian and Taiwanese Culture 315

6.8 Summary of this Chapter 315

7 Conclusion 320

7.1 Overview of this Chapter 321

7.2 Culture of Australian Computer Forensic Results 322

7.2.1 Australian Data Collection 322
7.2.2 Australian Outcomes of the Current Situation Dimension 323
7.2.3 Australian Outcomes of the Policy and Organization Dimension 324
7.2.4 Australian Outcomes of the Education Dimension 324
7.2.5 Australian Outcomes of the Law Dimension 325
7.2.6 Australian Outcomes of the Personal Preferences and Skills Dimension 325
7.2.7 The Relationship between the Australian Results and the Research Questions 325

7.3 Culture of Taiwanese Computer Forensic Results 327

7.3.1 Taiwanese Data Collection 327
7.3.2 Taiwanese Outcomes of the Current Situation Dimension 328
7.3.3 Taiwanese Outcomes of the Policy and Organization Dimension 328
7.3.4 Taiwanese Outcomes of the Education Dimension 329
7.3.5 Taiwanese Outcomes of the Law Dimension 329
7.3.6 Taiwanese Outcomes of the Personal Preferences and Skills Dimension 330
7.3.7 The Relationship between the Taiwanese Results and the Research Questions 330

7.4 Results of Major Research Question and Interpretations for Cross-Cultural Applications of Computer Forensics 332

7.5 Suggestions for Cross-Cultural Cooperation between Australia and Taiwan 334

7.5.1 Suggestions for Australian Computer Forensic Experts 335
7.5.2 Suggestions for Taiwanese Computer Forensic Experts 337
7.5.3 Suggestions for Australian and Taiwanese Computer Forensic Experts by Dimensions 339

7.6 Future Works 341

7.7 Conclusion to Research 342

8 Reference 344

Appendix 1: First Round Questionnaire for Delphi Survey in Australia (English Version) 370

Appendix 2: Second Round Questionnaire for Delphi Survey in Australia (English Version) 374

Appendix 3: The Results of First Round Questionnaire for Delphi Survey in Australia (English Version) 382

Appendix 4: The Results of Second Round Questionnaire for Delphi Survey in Australia (English Version) 404

Appendix 5: First Round Questionnaire for Delphi Survey in Taiwan (Chinese Version) 410

Appendix 6: Second Round Questionnaire for Delphi Survey in Taiwan (Chinese Version) 414

Appendix 7: Second Round Questionnaire for Delphi Survey in Taiwan (English Translation) 423

Appendix 8: The Results of First Round Questionnaire for Delphi Survey in Taiwan (Chinese Version) 432

Appendix 9: The Results of First Round Questionnaire for Delphi Survey in Taiwan (English Translation) *464*

Appendix 10: The Results of Second Round Questionnaire for Delphi Survey in Taiwan (Chinese Version) *495*

Appendix 11: The Results of Second Round Questionnaire for Delphi Survey in Taiwan (English Translation) *504*

Appendix 12: Case Study Questionnaire in Australia (English Version) *512*

Appendix 13: Case Study Questionnaire in Taiwan (Chinese Version) *514*

List of Figures

Figure 1: Derivation of Motivation..... 19

Figure 2: The Correlation among Original File, Normal Copy, and Bit Stream Copy 40

Figure 3: Classification of Computer Forensic Procedures..... 42

Figure 4: Concept of Computer Forensic – Secure, Analyse, Present Model 45

Figure 5: The Concept of Iterative Phases in Enhanced Integrated Digital Investigation Process Model 54

Figure 6: The Relationship among Electronic Crime Scene Investigation – A Guide for First Responders, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, and four conceptual phases 56

Figure 7: The Structure of Electronic Crime Scene Investigation – A Guide for First Responders 57

Figure 8: The Structure of Forensic Examination of Digital Evidence: A Guide for Law Enforcement 62

Figure 9: Modified Delphi Processes..... 127

Figure 10: The Triangulation of Research Methods in Australia 218

Figure 11: The Triangulation of Research Methods in Taiwan 289

List of Tables

Table 1: Digital Forensic Research Workshop Model *47*

Table 2: Hofstede's Scores for Australia and Taiwanese cultures *94*

Table 3: Corroborations for Hofstede's Five Cultural Dimensions *96*

Table 4: Different Axioms between Quantitative and Qualitative Research *104*

Table 5: Comparisons of Quantitative Research and Qualitative Research *105*

Table 6: The Comparison of Conventional Terms and Alternative Terms *112*

Table 7: Advantages and Disadvantages of Different Data Sources *146*

Table 8: Condition of Consensus and Agreement of Each Question within Current Situation Dimension *159*

Table 9: Condition of Consensus and Agreement of Each Question within Policy and Organization Dimension *160*

Table 10: Condition of Consensus and Agreement of Each Question within Education Dimension *161*

Table 11: Condition of Consensus and Agreement of Each Question within Law Dimension *161*

Table 12: Condition of Consensus and Agreement of Each Question within Personal Preferences and Skills Dimension *162*

Table 13: Relationships between Case Study Questions and Delphi questions *220*

Table 14: Condition of Consensus and Agreement of Each Question within Current Situation Dimension *230*

Table 15: Condition of Consensus and Agreement of Each Question within Policy and Organization Dimension *231*

Table 16: Condition of Consensus and Agreement of Each Question within Education Dimension *232*

Table 17: Condition of Consensus and Agreement of Each Question within Law Dimension *232*

Table 18: Condition of Consensus and Agreement of Each Question within Personal Preferences and Skills Dimension *233*

Table 19: Relationships between Case Study Questions and Delphi questions *291*

Table 20: Characteristics of Australian Culture and Taiwanese Culture *315*

Acronyms and Abbreviations

ACPO	Association of Chief Police Officers
ACSE	Australian Case Study Expert
ADFM	Abstract Digital Forensics Model
AFP	Australian Federal Police
C2	Command and Control
CFSAP	Computer Forensic – Secure, Analyse, Present
CIB	Criminal Investigation Bureau
CISSP	Certified Information Systems Security Professional
CPU	Central Police University
CS	Computer Science
CVS	Chinese Value Survey
DFRWS	Digital Forensic Research Workshop
EIDIP	Enhanced Integrated Digital Investigation Process
FBI	Federal Bureau of Investigation
IACIS	International Association of Computer Investigative Specialists
ICT	Information and Communication Technologies
IDIP	Integrated Digital Investigation Process
IISFA	International Information Systems Forensics Association
IS	Information Systems
MJIB	Ministry of Justice, Investigation Bureau
MRVS	modified version of Rokeach Value Survey
NIFS	National Institute of Forensic Science
NIJ	National Institute of Justice
SAPOL	South Australia Police
SOPs	Standard Operating Procedures
SWGDE	Scientific Working Group on Digital Evidence

TCSE	Taiwanese Case Study Expert
TWCERT/CC	Taiwan Computer Emergency Response Team/ Coordination Centre
UniSA	University of South Australia

1 Introduction

1.1 Introduction of this Thesis

The last two decades has seen a massive shift in consumer electronic devices, and devices that were once science fiction are now commonplace. Digital devices such as computer workstations, notebook computers, mobile phones, and digital cameras have become an accepted part of everyday lives. Their use, in conjunction with the global communications mediums such as the Internet has seen people connected in ways that were inconceivable in the past. With this rise in use of technology and instant communications comes its misuse, either to take advantage of flaws in protocols or the device itself, or as a means of facilitating further crimes. Traditional means of criminal and civil investigations are no longer appropriate to deal with computer-based crimes or crimes utilising computers as potential sources of evidence.

The investigation of crimes that involve digital devices and communications requires new processes and technologies, so as to provide a means of analysing all data in such a way to give an accurate account of what has occurred on a system and also to ensure that the outcome of an investigation is legally acceptable. This process is one of the major outcomes of the field of *Computer Forensics* (Cooper 2005; Francia 2006; Li and Seberry 2003; McKemmish 1999; Mercuri 2005; Patel and Ciardhuain 2000; Slay *et al* 2004; Wilsdon and Slay 2005). The term '*forensics*' refers to finding evidence for the '*trier of fact*', or for the court. Thus, computer forensics can be considered as finding computer-based evidence (digital evidence) for the '*trier of fact*', or for the court (this is discussed further in Section 2.2).

Since the use of digital equipment is an increasing societal trend, the consequent issues become unavoidable. This gives computer forensics a cogent reason to exist and to become a topical subject. Pollitt (1995a) provided similar argument around 12 years ago. Pollitt (1995a) said "*The preceding has been based on the use of computer forensics to exploit stored digital information. Certainly, this need will grow dramatically in the future, as more and more of society's information are stored electronically.*". With no doubt, Pollitt's statement agreed that the need for computer forensics will grow dramatically. This is an unavoidable trend for a contemporary society.

As part of this research, a consistency of terminology must be provided to enable a clearer understanding of the field. There are numerous names for digital information

forensics, such as forensic computing, digital forensics, cyber forensics, and computer forensics. Accordingly, within this research, the term '*computer forensics*' is used to represent forensics for electronically-stored information in order to minimize the confusions and/or misgivings. However, the researcher cannot guarantee the usage of other words by other scholars. Thus, readers may discover other terms, as listed above, which also mean computer forensics, when references are used, to ensure that the original author's words are transcribed accurately. However, for the purposes of this work, the terms are used with a common meaning, and are therefore interchangeable.

A review of Information Systems (IS) and Computer Science (CS) research over the last ten, or even twenty years shows an ever developing interest in, and concern about, the role that '*culture*' plays in the design and engineering of complex Information and Communication Technologies (ICT) systems. This concern extends to both the technological aspects of the systems and the human players, the users and developers, who play major roles. Examples of research questions that have been tackled include those contextualised within:

- Organisational and national culture, software specification and requirements analysis (Finkelstein and Fuks 1989)
- Human Computer Interaction - Culture and interface design (Cagiltay 1999)
- Cohesiveness of distributed teams working in a technologically mediated manner across national boundaries (Rathod and Miranda 1999; Vogel *et al* 2001)
- Cultural differences in virtual software teams (Dafoulas and Macaulay 2001)
- Cross-cultural perspectives within military ICT development (CCRP 2001, Slay 2001)

In addition, according to Slay and Quirchmayr (2004), Straub *et al* (2002) have a wide range of research outputs which point to the fact that "*it is the lack of clear concepts which makes cross-cultural research in the engineering of complex information systems difficult to conduct, and also links the effect of this lack of clarity to our inability to 'develop and refine theories' and to explain why there is difficulty in explaining the high degree of variance in current predictive models.*". Slay and Quirchmayr (2004)

further stated that "*It is recognised (Straub et al 2002) that cross-cultural work in technological disciplines 'remains in its infancy' because of the lack of unanimity about the underlying meaning and definition of the underlying construct 'culture'.*".

In short, this work thus builds on the work of Straub, Slay, Hofstede and many others to examine, once again, the role that culture plays in the broad area of IS – this time contextualised in the cross-disciplinary domain of computer forensics, which itself draws on computer science, electronic and telecommunications engineering, systems engineering, justice studies and law (among many others).

1.2 Aim of this Research

This research examines the effect of culture on computer forensics practices and processes and it does this by comparing and contrasting computer forensics issues, including issues of the current computer forensic workplace situation, policy and organization, education, law, and practitioners' personal preferences and skills, in Australia and Taiwan. Australia and Taiwan are chosen as examples of two of the very different and distinctive cultural variations found in the Asia Pacific. The differences between Australian and Taiwan can be found in Table 2. To do so, it uses a qualitative research methodology. The research output is a framework to guide Australian law enforcement, the Australian forensic science community and the courts in the implications of cross-cultural, cross-border and collaborative digital forensic investigations in the Asia Pacific. This research has the potential to help Australian forensic computing investigators in understanding how Taiwanese investigation methodologies, processes and procedures and legislative guidelines operate, and vice versa.

1.3 Research Motivation

Pragmatically, this research is motivated by discussion with Australian computer forensic professionals who have commented on the cultural difficulties that have arisen in their work in Asia. Theoretically, since there is a large body of research linking science and culture, and an equally large body examining information systems and culture, this research then seeks to establish a similar body of knowledge linking computer forensic (science) and culture, which is shown in Figure 1.

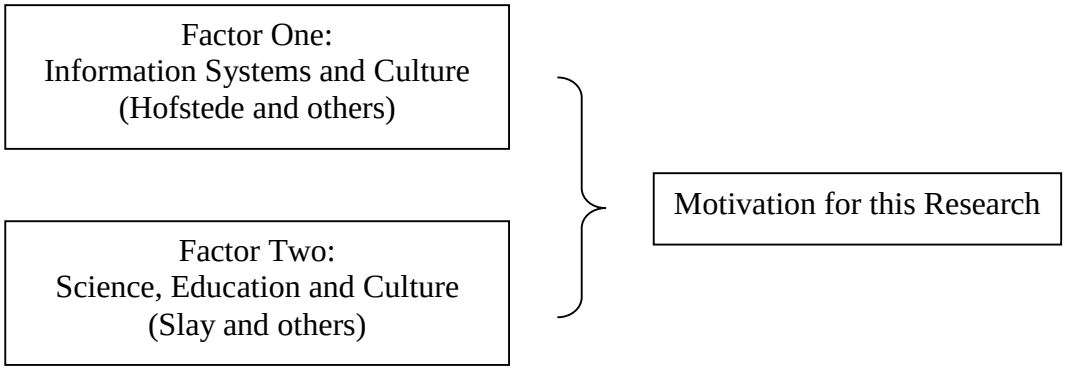


Figure 1: Derivation of Motivation

The novel perspective provided by this thesis is that issues of computer forensics are examined from a cultural perspective. To the researcher's best understanding, there is no similar academic work.

This concept is derived from work on IS and Culture, and particularly Hofstede's works (Hofstede 1986; Hofstede 1993; Hofstede 1994) and Slay's works carried out linking Science, Education and Culture (Slay and Kearney 2000; Slay and Burke 2001; Slay 2001; Slay 2002). These works not only point out that culture is not universal, but also demonstrate that different cultures are able to affect applications of science and thus infer that culture is a significant factor which may have the ability to affect computer forensic applications. Their works are discussed in detail in the Section 2.3.4.

Hofstede's works focused on the issue of national cultures, and proved that differences between national cultures and decision making indeed exist by using five national cultural dimensions. The detailed explanation of national culture can be found in the Section 2.3.4.2.1. Although his works are based on management issues, his contribution is that he examines the effect of culture on decision making. His works have been extensively referenced by other research (Kedia and Bhagat 1988; Erez and Earley 1993; Shore and Venkatachalam 1995).

1.4 Research Question

Therefore, the ultimate intention of this thesis is to use historical data, Delphi technique and case study interview to find out the answers to the research hypothesis. The research question is listed as follows:

In summary, the research question of this thesis is '*Does Culture have an impact on Computer Forensics Processes and Applications?*'.

Based on the research question, several sub-questions need to be discussed as well.

1. Does culture have an impact on current conditions of computer forensics?
2. Does culture have an impact on policy and organization of computer forensics?
3. Does culture have an impact on education and training within computer forensics?
4. Does culture have an impact on legal issues of computer forensics?
5. Does culture have an impact on the personal preferences and skills of computer forensic practitioners?

1.5 Research Limitations

This research is based on the results of a Delphi survey and two case studies per culture examined. Delphi survey is especially suitable for this research for two reasons. The first reason is that every respondent in a Delphi survey is an expert in the computer forensic field. The second reason is that Delphi survey provides a good opportunity for the respondents to express their thoughts. The results of a Delphi survey not only can reflect what are in the respondents' minds, but also become an effective way to represent the culture to which they belong. This concept was discussed by Hofstede and Bond (1988); they stated that "*Culture's grip on us is complete.*" Thorough discussion of the Delphi method can be found in the Section 3.5. Thus, it can be concluded that the Delphi is a useful method for examining the effect of culture. Sadly, this is also the limitation of this research. Respondents can freely express what is in their minds. The information that they provide may not be completely correct but is a personal interpretation derived from a chaotic work situation. Fortunately, this indicates as long as the majority of respondents have derived similar answers from their experience then the consensus is precise and valuable.

On the other hand, a case study gives a respondent a better opportunity to provide in-depth opinion on computer forensic issues. However, there are only two respondents in each of Australian and Taiwanese cultural settings under examination. This is because performing case study interviews costs time for both researcher and respondents. Most of respondents in the field of computer forensics have heavy work loads and inadequate time available.

The quality of this thesis is ensured by confirming its credibility, which is the alternative term for internal validity. The relationship between credibility and validity is discussed in Section 3.4.4. Moreover, the reason for using such alternative terms in qualitative research is discussed in Section 3.4. Lincoln and Guba (1985) and Patton (2001), interpret the dependability of qualitative research, which is the alternative term for reliability, as the consequence of the validity in a qualitative study. They are stating that as long as the credibility of this thesis is confirmed, the dependability is then ensured.

However, the generalization and the reproducibility of this thesis cannot be guaranteed, since these two factors are not suitable for this thesis. This research places emphasis on the impact of the cultural differences between Australia and Taiwan on the field of computer forensics. Due to the individuality of different cultures, the results of this thesis are very unlikely to apply to other cultures. This means that the concept of generalization cannot be achieved in this thesis. Generalization issues are further discussed in Section 3.4.4.2. Moreover, unlike quantitative research, the reproducibility of this thesis cannot be assured either. This is because the rapid development of computer forensics may change the attitudes of computer forensic experts. What is not acceptable yesterday may become acceptable today due to newly developed techniques and/or changed situations.

In short, the limitations of this research are the limited number of computer forensic experts, the inability to generalize this research over a long period of time or in other cultures, and the reproducibility of this research within other cultures.

1.6 Summary of this Chapter

This chapter introduces the topic that is the subject of this thesis – Computer Forensics – and explains how this discipline has grown enormously in the last ten years. It situates computer forensics within IS research and explains that there is a need to discover how culture impacts the computer forensic process from a human and technological perspective.

In order to answer the major research problem presented in this thesis, Delphi technique and case study interview are used both in Australia and Taiwan to elicit expert knowledge and are analysed within a recent-historical understanding of culture from IS and Science education research.

There are some limitations to this research. For example, the major restriction is that the inability to generalize this research over a long period of time or in other cultures. In summary, this thesis adopts Delphi technique and case study to establish the relationship between culture and applications of computer forensics, and focuses on the conditions occurring in Australia and Taiwan.

2 Literature Review

2.1 Overview of this Chapter

Within academic research, there are several aims of the Literature Review; to provide a succinct and relevant background to readers who may be unfamiliar with the current work in the research domains, to analyse current work in these areas as they are relevant to this research for comparative reasons, and to determine the academic and practical needs of investigation into the research problem. In essence, one of the greatest outcomes is to ensure the need of the research.

Since the topics, including computer forensics and culture, of this research are cross-disciplines, this chapter uses two sub-sections to explain the current situation of computer forensic issues, and the latest condition of cultural problems. In the Section 2.2, the concept of computer forensics is introduced. This is necessary because understanding computer forensics is fundamental for further discussions. In addition, the introduction of digital evidence can be found in this sub-section (Section 2.2.2.3) as well. This is because the purpose of computer forensics is to present relevant digital evidence within a court of law. Thus, it is common to consider that digital evidence plays an important role in the realm of computer forensics, and to regard that they are two topics which are closely related to each other. In Section 2.2.5, this thesis shows that the computer forensics is one of the subjects within the field of science. This infers that computer forensics is a branch of science. Academic researchers sometimes use the term, *Forensic Science*, to describe computer forensics. This standpoint is especially important to this thesis, since this is the critical point for the researcher to build the link between culture and science applications.

Moreover, the Section 2.3 not only discusses the definition of the culture, but also provides the concrete link between culture and science applications. The works conducted by Slay and Hofstede are perfect examples to show that the culture and science applications are not two mutual exclusive matters. Actually the culture and science applications are two topics which are closely related to each other.

In short, the literature starts by discussing computer forensics and culture respectively, and ends by showing that the science applications are affected by different cultures. Since computer forensics is a subject within the field of science, the link between culture and computer forensics is then established. Therefore, it can be inferred that culture must have specific effects on computer forensics. This is the major concern of

this thesis, and will be investigated using a Delphi questionnaire and case study interviews.

2.2 Computer Forensics

2.2.1 Overview of this Section

People have begun to deeply rely on and accept new technologies. The increasing use of electronic equipment (e.g. computer, laptop, mobile phone, digital camera, and personal digital assistant) is an example. People can communicate ubiquitously, and they can work more efficiently. The advantages brought by new technologies may be offset by the criminal use of these latest technologies to carry out crimes or illegal activities, or to use their security flaws to harass or victimise legal users. This means that new technologies and new electronic products pose new challenges for law enforcement in conducting of investigations The field of investigation that analyses and investigates digital evidence has a number of names, one of which is computer forensics (Cooper 2005; Francia 2006; Li and Seberry 2003; McKemmish 1999; Mercuri 2005; Patel and Ciardhuain 2000; Slay *et al* 2004; Wilsdon and Slay 2005). The purpose of this field is to solve problems brought by the involvement of digital products in a crime or as a result of some misuse.

Section 2.2.2 of this research introduces discussion to determine the definition of computer forensics, the purpose of the field, the definition of digital evidence, and the characteristics of digital evidence. In Section 2.2.3, procedures of computer forensics are introduced. Standard Operating Procedures (SOPs) are especially important for this research, as they provide the underlying fundamental principles from which this work is based. This is particularly true as different cultures are likely to have different standpoints for computer forensic procedures. In Section 2.2.4 of this research explores the current operational and research issues and predicaments for the field of computer forensics. This section is particularly significant in that the research domain of computer forensics is a relatively young subject. Because of this reason, basic standards are not properly refined or applied. Thus, certain limitations exist and these limitations are important factors in evaluating the diverse perspectives of different cultures. Lastly, Section 2.2.5 concludes the component of the literature review discussing computer

forensics, and makes a final argument to determine whether computer forensics is a form of science, or relies on scientific underpinnings.

2.2.2 What is Computer Forensics?

Whilst in practical terms the field of computer forensics essentially is the investigation and analysis of digitized data, where the arbitration may be suitable for court or tribunal, there are several intricacies and discussions, both from an operational and academic perspective, that detail the limitations, scope and boundaries of this area. An in-depth understanding of the field of computer forensics and its accompanying issues is the foundation of this thesis, and therefore a consistent definition must be chosen for the term, as this potentially impacts upon several areas of this work.

This section is broken down into 5 sub-sections; first, the definition of the term C*omputer Forensics* is discussed, along with several alternate but similar terms, such as *Digital Forensics*, and *Forensic Computing*. Beyond this, the definition of computer forensics is introduced in Section 2.2.2.1. In Section 2.2.2.2, this thesis presents the purpose of computer forensics. In addition, the introduction, definition, and traits of digital evidence are presented in Section 2.2.2.3, Section 2.2.2.4, and Section 2.2.2.5 respectively.

2.2.2.1 Definition of Computer Forensics

Before any further discussions of computer forensics, the definition of this field must be clarified and discussed. In this section, several definitions of computer forensics are listed. Through analysis of these definitions, a single definition, appropriate for this work, can be reached. This section discusses and compares these definitions to determine the most appropriate one for this thesis.

Pollitt (1995a) provided one of the earliest definitions for the field, and stated that "*Computer forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law. At one extreme is the pure science of ones and zeros. At this level, the laws of physics and mathematics rule. At the other extreme, is the courtroom.*". This definition is pioneering in that it encompasses both the process and possible outcomes of computer forensics, explicitly that analysis of

computers is the aim but that all outcomes must be legally acceptable. However, this definition is also cumbersome and dated in several ways. Describing computer forensics as '*a synthesis of science and law*' is necessarily vague for both the definitions of the terms '*science*' and '*law*', as any computer forensic process would only encompass a subset of scientific process. The definition put forward by Pollitt (1995a) similarly is vague about the outcomes at the courtroom. This term does not consider the gamut of other arbitration and legal aspects, rather that computer forensic outcomes need not end up in a courtroom, but be legally acceptable. Therefore, whilst the definition developed by Pollitt (1995a) was at the time groundbreaking, it is not succinct and seems dated based on definitions that have since emerged.

McKemmish (1999) described the concept of forensic computing in the following manner: "*forensic computing which is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.*". Although the definition of computer forensics provided by McKemmish is very concise, this definition indeed provides necessary information for people to understand the essential meaning of computer forensics. McKemmish used four major processes to express the core concept of computer forensics, and stated that the product of these processes, digital evidence, must be legally acceptable. His definition infers that computer forensics is a multi-disciplinary subject, and its contribution is that this definition is the earliest definition provided in Australia. In addition, McKemmish's definition is also interesting in that it explicitly notes that the presentation is a component of the process, which is not stated in the same way in the work of Pollitt (1995a).

Palmer (2001) gave the definition of computer forensics as "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.*". This definition was developed in the Digital Forensic Research Workshop (DFRWS), and was based on a consensus made by attending academic researchers. The consensus of attending academic researchers infers that most biases are ruled out, and the quality of this definition of computer forensics is that it is reliable and trustworthy and was agreed to by reading researchers in the field at the time when DFRWS met for the first time.

The previous three definitions of computer forensics all show that computer forensics is an activity containing legal issues and technical perspectives. The success of computer forensics needs cross-disciplinary cooperation. Moreover, this standpoint is supported by other academic researchers. For example, Patzakis (2003) asserted that the meaning of computer forensics as "*Computer forensics is a mandatory process whenever the results of a computer investigation may ultimately be presented in a legal or administrative proceeding.*". Volonino (2003) provided a simpler explanation of computer forensics as "*Computer forensics is the search of computer and communication devices for existing or deleted e-evidence, the abbreviation of digital evidence.*". These two definitions may not provide explicit and specific explanations for computer forensics, but they do point out that computer forensics is a multi-disciplinary issue containing legal and technical perspectives.

Given the current discussion, this research will use the definition of computer forensics as proposed by Palmer, that computer forensics is: "*The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.*" (Palmer, 2001).

There are several reasons for this choice. The first reason is that whilst this definition is similar and in context with the other definitions presented, it defines well the processes involved in the field to a larger degree than most. Whilst there are other, similar definitions, such as those proposed by McKemmish (1999) and Pollitt (1995a), these do not have the granularity in the process model as given by Palmer. However, this definition is easily mapped to these other definitions and they all address a common theme. Also, as the definition was developed in the DFRWS by the best and well-known academic researchers at that time, there can be little doubt to the reliability and acceptance of this work.

2.2.2.2 Purpose of Computer Forensics

As given by the definition used for this research, the field of computer forensics forms part of an investigation into misuse, and the outcomes of this must be acceptable within

a court of law or arbitration process. Therefore there is a heavy reliance upon the non-technical areas of the field, given its multi-disciplinary nature. As given by Yasinsac *et al* (2003), this misunderstanding can be clarified, as "*computer forensics is multidisciplinary by nature, due to its foundation in two otherwise technologically separate fields (computing and law).*". Given the multi-disciplinary nature of computer forensics, a definition of the purpose of computer forensics must be discussed and well-explained to give context to this thesis. There are several academic and practitioner-based definitions for computer forensics listed below, so as to show the importance of the purpose of computer forensics.

Pollitt (1995a) originally defined the field of computer forensics with the following quote: "*To get something admitted into court requires two things. First, the information must be factual. Secondly, it must be introduced by a witness who can explain the facts and answer questions. While the first may be pure science, the latter requires training experience, and an ability to communicate the science*". Additionally, the author said that "*The process used must conform to both the law and science. Failure in either arena, renders the product legally worthless.*". Pollitt (1995b) expanded upon this concept and said "*investigators and others have, by trial and error, evolved methods which will allow the discovery of evidence from storage media that will satisfy the twin requirements of science and law.*". Therefore, Pollitt saw that computer forensics not only as requiring technical skills, but also legal skills, and that the final outcomes of the field are geared towards a legal or arbitration framework.

There has been discussion and research in academia that has sought to quantify and highlight the purpose and outcomes of computer forensics as a discipline, and many of these have drawn upon the earlier work of Pollitt (1995b). In particular, Civie and Civie (1998) stated that the working definition of computer forensics as "*The pursuit of knowledge by uncovering elemental evidence extracted from a computer in a manner suitable for court proceedings.*". Whilst the similarities here are striking, the key differences lie in the terms *elemental evidence* and *suitable for court proceedings*. Civie and Civie (1998) describe the word *elemental* as being based on the physical characteristics of a device, and this is interesting in that it therefore relates solely to low-level analysis, and has limited logical and high-level applicability. Also, the terminology *suitable for court proceedings* is unintentionally inclusive, as it relates only

to a ‘court proceedings’ outcome, rather than any number of other arbitration or military investigations that may occur.

Besides the above arguments on the purpose of computer forensics, there are more authors who discuss this issue. For example, Bates (1998) stated that “*The purpose of forensic investigation is to enable observations and conclusions to be presented in court.*”. Forte (2003) stated “*The simple guiding principle universally accepted both in technical and judicial spheres, is that all operations have to be carried out as if everything will one day have to be presented before a judge.*”. Meyers and Rogers (2004) identified that “*computer forensics is in the early stages of development and as a result, problems are emerging that bring into question the validity of computer forensics usage in the United States federal and state court systems.*”. According to Solon and Harper (2004), “*computer-based digital evidence is very fragile; it can be easily altered, damaged or destroyed by improper handling. If the data have not been dealt with correctly, the judge will not allow it to be used in legal proceedings.*”. Pan and Batten (2005) stated “*In order to be usable as evidence in a court of law, such information needs to be captured in a systematic way without altering it in so doing. Thus, the process of identification and handling of the evidence is of prime concern in a forensic investigation.*”. One common feature of these authors is that they all state that the ultimate goal of computer forensics is to provide legitimate and correct digital evidence in a court of law rather than merely examining digital equipment or analysing digital data. From this, it is realized that computer forensics is not a subject that is entirely comprised of technical issues, but it is a discipline containing both computer techniques and legal issues.

In order to present forensically sound digital evidence in a court, computer forensic investigators must follow strict procedures, such as the *Good Practice Guide for Computer based Digital evidence*, a guide developed by the Association of Chief Police Officers (2003) (ACPO). This regulatory guide states that interaction with devices that may contain digital evidence should be avoided. All interaction that may alter the state of digital evidence should be avoided. By adhering to these guidelines, computer forensic investigators can ensure that the gathered digital evidence is forensically sound, and avoid the reliability problems of digital evidence caused by improper handling procedures.

From these discussions, it can be seen that the domain of computer forensics is based on multiple disciplines. This situation raises two serious issues. The first concern is that computer forensic practitioners must be trained properly to gain the appropriate technical skills. They must understand sophisticated technical issues in the computer forensic field, and also scientific solutions for retrieving digital data in order to produce evidence for a court. In addition, the second concern is that they have to recognize the corresponding legal problems which may caused by performing computer forensic actions or simply in the usage of digital evidence. They, therefore, can avoid any possible attacks from the defendant's lawyer about the validity, trustworthiness, and legitimacy of the digital evidence.

To summarise, since the essential goal of computer forensics is to provide legitimate digital evidence for a court or other similar panel, the primary consideration of computer forensic examiners is the trustworthiness of the digital evidence. Trustworthiness is the fundamental property of digital evidence when it is presented within a court of law.

2.2.2.3 Introduction of Digital Evidence

There are numerous names for electronically-stored information, such as digital evidence (Porada and Straus 2007; Richard III *et al* 2007) and e-evidence (Liophanich 2005a; Liophanich 2005b). This is a similar situation to the diverse terms for computer forensics. Different scholars use different terms to represent and to discuss the same issue. In this thesis, the term, *Digital Evidence* (Scientific Working Group on Digital Evidence 1999), is used to represent electronically-stored information in order to minimize confusions and/or misgivings. However, the researcher cannot manipulate the usage of other terms by other scholars. Thus, readers may find other terms, which also mean electronically-stored information, when references are used.

Since the initial purpose of computer forensics is to provide legitimate, valuable, and compelling digital evidence for a court, the role of digital evidence is explicitly important in the realm of computer forensics. Wang (2007) provided a remarkable insight to depict the characteristic of digital evidence. He stated that "*The difference between digital evidence and physical evidence is that each examining action would be treated as 'Access' in the collection of digital evidence, as it is easy to change the*

content of digital evidence and so disqualify the criminal facts.". According to this statement, it is realized that the nature of digital evidence is volatile. In addition, this also infers that the features of digital evidence are very different from the characteristics of physical evidence.

Barbara (2005) said the main difference between digital evidence and physical evidence is "*...there is no actual 'physical evidence' in the traditional sense to visually collect. The evidence is digital, consisting of '0's' and '1's', which cannot be seen by the naked eye for relevance or collection purposes.*". The purpose of this statement explains that digital evidence cannot be read and understood by human. This infers that interpretation by equipment and/or software is necessary for understanding digital evidence. This standpoint is also confirmed by the definition of digital evidence, provided in the National Institute of Justice (2001b), which depicted as "*Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence are latent. In its natural state, we cannot 'see' what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence visible. Testimony may be required to explain the examination process and any process limitations.*". The major characteristic of digital evidence then is that it cannot be directly interpreted and understood by humans. Professional equipment and technical skill is required to interpret the original digital evidence.

From these definitions, it can be seen that digital evidence is different from traditional evidence, such as physical evidence, and has unique characteristics. Unlike conventional evidence, digital evidence has the potential to be modified either inadvertently or intentionally.

This section has also raised the issue that digital evidence differs from traditional evidence in that it can often be replicated completely. In addition, integrity is also a potentially serious issue with digital evidence, as integrity is related to the effectiveness of the digital evidence within a court of law. Correct and established collection procedures are designed to maintain the integrity of digital evidence. This section has also shown that one of the major outcomes of digital evidence and the forensic process is in the outcomes. Digital evidence cannot be perceived by individuals, since it consists

of '*0's*' and '*1's*'. Thus, well-trained computer forensic examiners and valid computer forensic tools are essential for a computer forensic investigation.

Due to these unique features, it is quite a challenge for computer forensic investigators to properly preserve digital evidence. Thus, computer forensic investigators must follow certain well-defined procedures. The appropriate procedures not only can become a manual for other computer forensic investigators to follow, but also ensure the results are accurate, reliable, confirmable, and repeatable. Procedure issues are discussed in the Section 2.2.3. In the next two sections (Section 2.2.2.4, and Section 2.2.2.5), the definition, and traits of digital evidence will be introduced and discussed.

2.2.2.4 Definition of Digital Evidence

After preliminary explanations of digital evidence in the previous section, the introduction of its definition must be established in order to understand digital evidence properly. The definitions of digital evidence from different sources and different scholars are listed below.

Pollitt (1995a) provided a definition for digital evidence as "*One major area in which this is being felt is that of the acquisition, authentication, evaluation, and legal admissibility of information stored on magnetic and other media. This information can be referred to as digital evidence.*". This statement means that digital evidence has two main features. The first feature is that digital evidence must be accepted by a court of law, and the second characteristic is that digital evidence must be stored in digital form on digital media. Coincidentally, Volonino (2003) proposed a very similar account and stated that "*E-evidence is electronically-stored information on any type of computer device that can be used as evidence in a legal action.*". In addition, Casey (2000) proposed an analogous standpoint for digital evidence as "*Digital evidence - evidence that is stored on or transmitted by computers - can play a major role in a wide range of crimes, including homicide, rape, abduction, child abuse, solicitation of minors, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, espionage, and terrorism.*". The two statements, proposed by Volonino (2003) and Casey (2000), both provide a similar explanation for digital evidence, and also respond to the statement provided by Pollitt (1995a). In short, Pollitt (1995a), Volonino (2003),

and Casey (2000) all agreed that digital evidence is a concept which contains legal and technical perspectives.

Lastly, National Institute of Justice (2001b) stated that "*Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. Such evidence is acquired when data or physical items are collected and stored for examination purposes.*". This statement concerns the role of digital evidence from both legal and technical perspectives as well. For this research, the definition provided by the National Institute of Justice (2001b) is used as an 'official' definition of digital evidence. This definition was created by the United States of America government organization, which holds the leading position within the field of computer forensic research. In addition, no severe criticism of this definition and work has been found since its publication. This indicates that the reliability and completeness of this definition are well established.

2.2.2.5 Traits of Digital Evidence

It is worth noting that digital evidence is a completely different concept from physical evidence or conventional evidence. A typical and well-known characteristic of digital evidence is that digital evidence itself is very fragile. The state of digital evidence may be changed through turning on/off a computer. Mocas (2004) described the primary properties of digital evidence as *Integrity*, *Authentication*, *Reproducibility*, and *Non-Interference*. More characteristics of digital evidence are introduced in this thesis.

In this section, the meaning of metadata is explained first, since metadata is one of the most well-known and important characteristics of digital evidence. Several other features of digital evidence are also examined, such as the reproducibility of digital evidence, and time stamps within digital evidence.

2.2.2.5.1 Metadata

Several researchers have given discussion of metadata with definitions notably provided by Buchholz and Spafford (2004), Kenneally (2004) and Castigline *et al* (2007). Metadata can be considered one of the most well-known and important characteristics of digital evidence. An explicit explanation of metadata can be found in (Brilis *et al* 2001) as "*Metadata is data about data and consists of information that characterizes*

data. Metadata are used to provide documentation for data products. In essence, metadata answer who, what, when, where, why, and how about every facet of the data that are being documented.". Typical metadata used in the field of computer forensics includes time stamps and log files. Time stamping is used as example here and is further discussed in the next section (Section 2.2.2.5.2).

Metadata was not designed for forensic purposes and is a product of the operating system. However, metadata has the ability to provide additional information for computer forensic investigators. Thus, how to obtain correct metadata is of vital importance to computer forensic investigators. The use of metadata is exceptional in computer forensic analysis as there is no functional equivalent in other forms of evidence (e.g. paper-based evidence).

2.2.2.5.2 Time Stamp

Time stamps are an effective and valuable form of metadata, since they have the potential to indicate '*the time when does the change of a file occur?*' (Schatz *et al* 2006). These changes may the include creation or modification of a file. Schatz *et al* (2006) further wrote that "*Time stamps are increasingly used to relate events which happen in the digital realm to each other and to events which happen in the physical realm, helping to establish cause and effect.*". This statement shows that time stamping is the means whereby useful digital incidents may be linked to physical evidence in the real world. The importance of time stamp is thus paramount.

Time is one of the critical factors to establish the validity of digital evidence. The powerful argument as stated by Gladyshev and Patel (2005) is "*If event A caused event B and event B caused event C, then the time of B must be between the times of A and C. This type of reasoning is sometimes called event time bounding.*". Readers can understand from the statement made by Gladyshev and Patel that the computer forensic investigators may not know the exact time of event B, but they still can judge an estimated time of event B by understanding the time of event A and the time of event C. This is very useful for computer forensic practitioners in their work, since they can utilize the causality of events to decide the possible answers. The argument not only indicates that the time stamping of a digital event is very important, but also shows that the sequencing of digital events is one of the significant factors to determine the result

of a case. For example, a suspect may have an irrefutable alibi for times that the computer or digital devices were in use, and this may help to establish mitigating evidence. Other researchers confirm the importance of this issue; Gladyshev and Patel, Mocas (2004) also proposed a similar argument about the effects of time and Mocas (2004) also stated that time is the key factor to determine the sequence of events.

Ahmad (2002) stated that "*the link between each log is crucial to the establishment of a complete chain of evidence. A cross all of the links the crucial factor upon which the integrity of the entire chain rests is the authenticity of the time-line. If the accuracy of the time in any of the links is questionable then the entire chain is rendered useless.*". The essence of this statement is similar to the account provided by Gladyshev and Patel (2005). Time stamping, or time-lining, is an irreplaceable factor to establish the chain of evidence.

In addition, Stevens (2004) is another scholar who also agreed with this concept. He asserted that "*For digital investigations involving computers and other digital equipment, a time-line of events as recorded by the equipment may provide a critical piece of information that is vital for solving the crime.*". Based on this statement, it is realized that time stamps can offer additional information for confirming the relationship between digital events. Buchholz and Falk (2005) developed a tool called Zeitline to establish the order the events by their time values. They stated "*Searching for keywords, file types, or file hashes might be sufficient when trying to locate incriminating material on a system, but is insufficient when trying to reconstruct events that have taken place on a system. Zeitline allows a forensic investigator to construct and view a time line of events based on the information found the system under investigation.*".

Weil (2002) proposed a method called dynamic time and date stamp analysis to correlate times and dates in a file. His method indicates the significance of time in the realm of computer forensics as well. Hosmer (2002) also stated the importance of time line as "*Time as a quantified value is used in nearly all aspects of commerce and security in order to bind validity, grant access, and reconstruct the order of events.*". In summary, different academic researchers all provide similar understanding of the importance of time stamping or time-lining as factors for understanding the sequence of digital incidents within the field of computer forensics.

Another characteristic of time is that the concept of the time is crucial to the non-scientists (e.g. judges, lawyers, and jurors). Hosmer (2002) further said that "*Time essentially is an agreement that allows society to function in an orderly fashion – where all parties are able to easily understand the representation*". The statement provided by Boyd and Forster (2004) shows the same contention as "*Date and time evidence is a fundamental part of many forensic computing examinations. Forensic examiners know that lawyers are often drawn to dates and times because they represent a concrete link between the real world and the less easily understood world of computer evidence.*". The reason for this is because the concept of the time is the kernel of daily life. It is easy for lay people to understand the principle of how the time works and thus, as part of the court process, accurate time representation is necessary as part of the computer forensic process.

In short, the significance of the time stamp can be understood from the examples given – it is a means of establishing a known timeline from computer events. From a broader point of view, the time stamp not only indicates the time of a single event, but also gives the computer forensic investigators an ability to build the time-line of events. The sequence of the events is helpful to determine the innocence or guilt of the respondent. Moreover, time is a better way to help the non-scientists (e.g. judges, lawyers, and jurors) to understand the investigated digital incident.

2.2.2.5.3 Integrity

According to Mocas (2004), Landwehr (2001) provided the definition of data integrity as "*Assuring that digital information is not modified (either intentionally or accidentally) without proper authorization*". Moreover, Mocas (2004) redefined integrity as "*Assuring that, given a data set, the process of creating a duplicate of the data does not modify the data (either intentionally or accidentally) and the duplicate is an exact bit copy bit copy of the original data set.*". The statement made by Mocas not only described the definition of integrity, but also covered the meaning of reproduction. In addition, Duren and Hosmer (2002) provided a different perspective to achieve the integrity of digital evidence. They suggest using time stamps to ensure the integrity of digital evidence. Normally the integrity of digital evidence is protected and checked by a hash function. However, one thing worth noticing is that Forte (2003) proposed an interesting point stating that cryptography not only can guard the confidentiality of

digital evidence and/or communications between computer forensic investigators, but also can guarantee the integrity of digital evidence since no party can alter the encrypted information unless the party has corresponding decryption key.

In summary, the information provided in this section shows the importance of integrity of digital evidence. The purpose of the integrity of digital evidence can maintain the validity, reliability, and credibility of digital evidence within a court of law.

2.2.2.5.4 Authentication

National Institute of Justice (2001a) provided the definition of authentication as "*Sufficient to support a finding that the (computer record or other evidence) in question is what its proponent claims.*". Moreover, Mocas (2004) adopted the meaning of authentication from the computer security perspective as "*Knowing that the apparent author of text is in fact the true author.*". This indicates that the purpose of authentication is to ensure the connection between the data and the data originator.

From a computer forensics perspective, authentication relates to the relation between the digital evidence and its originator. Computer forensic investigators must ensure the authentication of evidence so as to build the correct and convincing link between the digital evidence and the corresponding originator. Since the digital evidence is going to be presented within a court of law then the provision of good and compelling evidence on au authentication is necessary for digital evidence to be useful to the court.

2.2.2.5.5 Reproducibility

The importance of reproducibility is provided in a statement made by Mocas (2004). Mocas (2004) explained the need of reproducibility in a scientific field as "*A key feature of science is that hypotheses are supported by reproducible experiments. Reproducibility strengthens the belief that a hypothesis is correct. Likewise, the reproducibility of investigative procedures lends credibility to the evidence produced.*". Then, Mocas (2004) further gave reproducibility a definition as "*Assuring that, given a data set or set of devices, the processes used to gather and/or examine evidence from the data set or devices are reproducible.*". The facts expressed by Mocas (2004) explain the meaning of reproducibility and show that the value of reproducibility in the scientific field. In addition, Pan and Batten (2005) gave a similar explanation of

reproducibility as "*the ability to achieve a consistent level of quality throughout the investigative process, no matter how many times it is repeated under the same conditions.*". The statements, provided by Mocas (2004) and Pan and Batten (2005), both agree that reproducibility is necessary to support and enhance the credibility and quality of the scientific outcomes.

In addition, reproducibility is a concept not only important in the scientific field, but also significant in the field of computer forensics. The concept of reproducibility within the field of computer forensics is slightly different from its scientific explanation. The reason for this can be found in Kenneally and Brown (2005), who discussed the importance of reproducibility by stating that "*The volatile nature of computer network and disk evidence and the potentially destructive nature of the analysis process make a convincing argument for investigators to not perform analysis on original evidence.*". This statement not only can be regarded as the major reason for computer forensic investigators to reproduce the original digital evidence, but also points out the demand of reproducing digital evidence. In this manner, computer forensic investigators have to take different approaches to find out necessary information within an investigation without the modification of original digital evidence. More discussion about reproducibility is provided below.

The concept of reproducibility within the field of computer forensics is also described by Bates (1998) as "*It is a fact that when such information is copied, there is no way to distinguish which is the original and which is the copy without reference to additional external information*". Bates's words infer that the copy version of a file is exactly the same as the original one. Reproducibility gives the computer forensic investigators an ability to examine the cases by using copy version of a file rather than the original one.

Furthermore, attention must be given to the word '*copy*'. The word '*copy*' in the field of computer forensics refers to bit stream copy rather than traditional copy. The differences between these two types of copy are shown in the Figure 2. Figure 2, which is referred from Wang (2007), not only demonstrates the correlation between original file, traditional copy, and bit stream copy, but also shows the difference between traditional copy and bit stream copy.

Original File	A	B	C (deleted)	D (deleted)	E
Traditional Copy	A	B	E		
Bit stream Copy	A	B	C (deleted)	D (deleted)	E

Figure 2: The Correlation among Original File, Normal Copy, and Bit Stream Copy

The capability of a bit stream copy was described by Kenneally and Brown (2005) as "*Bit-stream collection affords examiners the opportunity to freeze the entire scene as it exists on the seized disks, for offline static analysis. This methodology effectively compartmentalizes the processes of acquisition and analysis of digital evidence*". From this explanation, the importance of bit stream copy within the field of computer forensics can be understood. Bit stream copy is able to duplicate every bit that exists on the seized disk. This function is especially significant since the seized data needs to be presented in a court of law.

In addition, Wang (2007) further provided the advantage of bit stream copy and stated that "*Copying evidence stored inside the computer requires a special tool and must be carried out bit by bit; this is to say, the data must be copied using a bit-stream-copy method, which provides copied information in exactly the same format as the original data. By using this bit-stream-copy method, the data obtained are given more probative force. The most important thing is that the evidence is not amended or changed during the copying process*". Based on these explanations, it can be shown that there is no possibility for the original digital evidence to be changed, jeopardized, or modified during the computer forensic investigation if a bit stream copy method is used.

2.2.2.5.6 Non-Interference

As digital evidence is fragile, the concept of non-interference becomes extremely important within the field of computer forensics. The National Institute of Justice

(2000) discussed the rules of non-interference within a physical crime scene as "*One of the most important aspects of securing a crime scene is to preserve the scene with minimal contamination and disturbance of physical evidence.*" The concept of non-interference can be adopted for digital evidence also. The work from the National Institute of Justice (NIJ) infers that the best situation for a physical and/or digital crime scene is to maintain the scene as original as possible.

Mocas (2004) expanded upon this work and defined the non-interference of digital evidence as "*Assuring that the method (or tool) used to gather and/or analyse digital evidence does not change the original data set*". If the non-interference of digital evidence is ensured, the validity, credibility, and reliability of digital evidence is strengthened. This is a logical conclusion, given that digital evidence has a potential outcome to be presented within a court of law. Therefore, non-interference is a requirement in digital evidence.

2.2.3 Procedures of Computer Forensics

Procedures are an important and ongoing issue in the field of computer forensics. The quality, validity, and credibility of digital evidence are not only affected by computer forensics procedures, but also the accuracy of the outcomes of any work. This research debates the procedures for computer forensics and classifies these into two segments: research-based general processes and practitioner-based general processes. The research-based general models are discussed in section 2.2.3.1, and the practitioner-based general models are debated in the section 2.2.3.2. Moreover, the concept of the SOPs is introduced within section 2.2.3.3, since SOPs can be considered the ultimate achievement of these general models. Figure 3 shows the classification of computer forensic procedures in this thesis.

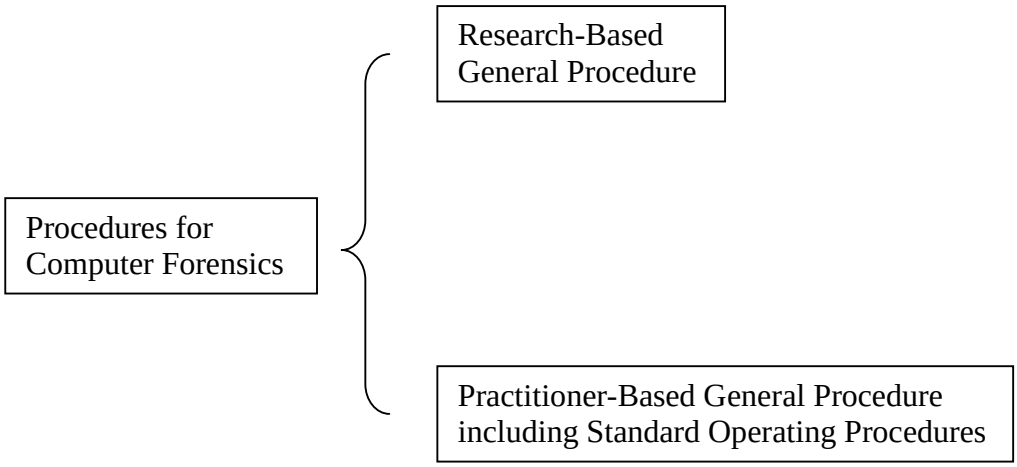


Figure 3: Classification of Computer Forensic Procedures

The benefit of general procedures for the field of computer forensics was described by Reith *et al* (2002) as "*This allows a consistent methodology for dealing with past, present, or future digital devices in a well-understood and widely accepted manner. For example, this methodology can be applied to a range of digital devices from calculators to desktop computers, or even unrealized digital devices of the future.*". In this case, the general procedures for computer forensics are flexible rather than limiting themselves to a particular process or usage. Reith *et al* also introduces a number of reasons that standard procedures are lacking in many operational laboratories. These reasons are; the uniqueness of a single case is not appropriate for SOPs, continually changing technologies require alternations to existing SOPs, and differing legislation and jurisdictions require flexible SOPs. The requirement to overcome these limitations raised by Reith *et al* is the flexibility discussed. Flexibility allows changes within a framework but with a formed overall outcome. However, such a flexible, and possibly non-detailed set of SOPs also needs a measure of detail, and it is therefore a fine balance to make. The most obvious advantage of a general process for computer forensics is that the process itself is flexible and changeable.

Baryamureeba and Tushabe (2004) have also discussed the importance of general processes in the field of computer forensics, stating that "*The process (methodology and approach) one adopts in conducting a digital forensics investigation is immensely crucial to the outcome of such an investigation. Overlooking one step or interchanging any of the steps may lead to incomplete or inconclusive results hence wrong interpretations and conclusions. A computer crime culprit may walk Scot-free or an*

innocent suspect may suffer negative consequences (both monetary and otherwise) simply on account of a forensics investigation that was inadequate or improperly conducted".

Baryamureeba and Tushabe proposed one important concept. They put emphasis on the general process for computer forensic investigations rather than focusing on SOPs in the field of computer forensics. Their idea showed that the significance of the general process is likely to affect the results of a case. Thus, development of a general process should be taken into serious account since the development of SOPs is currently an important area of research. A general process is currently the only method, or framework, that most computer forensic examiners can rely on when performing computer forensic investigations.

2.2.3.1 Research-Based General Procedures of Computer Forensics

There is considerable ongoing research into general procedures in computer forensics (Beckett and Slay, 2007; Lin *et al* 2003a). Research-based general procedures can be considered the foundation of the development of practitioner-based general procedures. With the efforts done in the development of research-based general models, it is much easier then to develop practitioner-based general models.

Continuing with the discussions proposed by Reith *et al* (2002) in previous section, Reith *et al* (2002) is not alone in discussing general procedures, or methods of partitioning the stages of a computer forensic investigation. The understanding of other scholars is discussed below:

McKemmish (1999) defined four major steps of a computer forensic investigation, which are:

1. ***The Identification of Digital Evidence***

   The purpose of identification of digital evidence is to know what is the potential digital evidence, to understand where the digital evidence is stored, and to recognize how the digital evidence is stored. In here, the source of digital evidence is not limit itself to computer. Any electronic devices can be considered the sources of digital evidence.

2. ***The Preservation of Digital Evidence***

   The purpose of preservation of digital evidence is to make sure the original status of the digital evidence. However, some changes are not avoidable under certain circumstances. In this case, the least amount of changes must be ensured, and the changes have to be explained properly.

3. ***The Analysis of Digital Evidence***

   The purpose of analysis of digital evidence is about extraction, processing, and interpretation of digital evidence. The major concept of this step is to translate binary data into humanly meaningful manner. This step can be considered the most important phase in the computer forensics.

4. ***The Presentation of Digital Evidence***

   The purpose of presentation of digital evidence is to actually present digital evidence in a court of law. The capability and the qualification of the presenter need to be accounted carefully at this phase.

In McKemmish's work, an investigation is divided into four stages. The first stage is to recognize the target, digital evidence. The second stage is to maintain the original state of the digital evidence. The third stage is to examine the content of digital evidence. The last stage is to present the digital evidence within a court. In the year of 1999, this classification can be considered a fundamental understanding of computer forensics since it was the beginning stage of the development of computer forensics. Computer forensics plays an awkward role at that time.

The work of McKemmish gave a clear direction of computer forensics investigations at an early period of its development. These steps provide a general concept for computer forensic examiners when an investigation proceeds. The generalized procedures from McKemmish are designed to focus on more than the technical elements and therefore have outcomes applicable to the outcomes of the field, and are therefore inclusive of judicial members (e.g. the judge, the lawyer, and the jury) without technical backgrounds. This indicates that McKemmish's work definitely shows a clear way for the future developments of the computer forensic process.

McKemmish later refined this work with input from several other authors. The outcome of this is Computer Forensic – Secure, Analyse, Present (CFSAP) model (Mohay *et al* 2003). The general concept of CFSAP model is displayed in Figure 4 (Turnbull 2007).

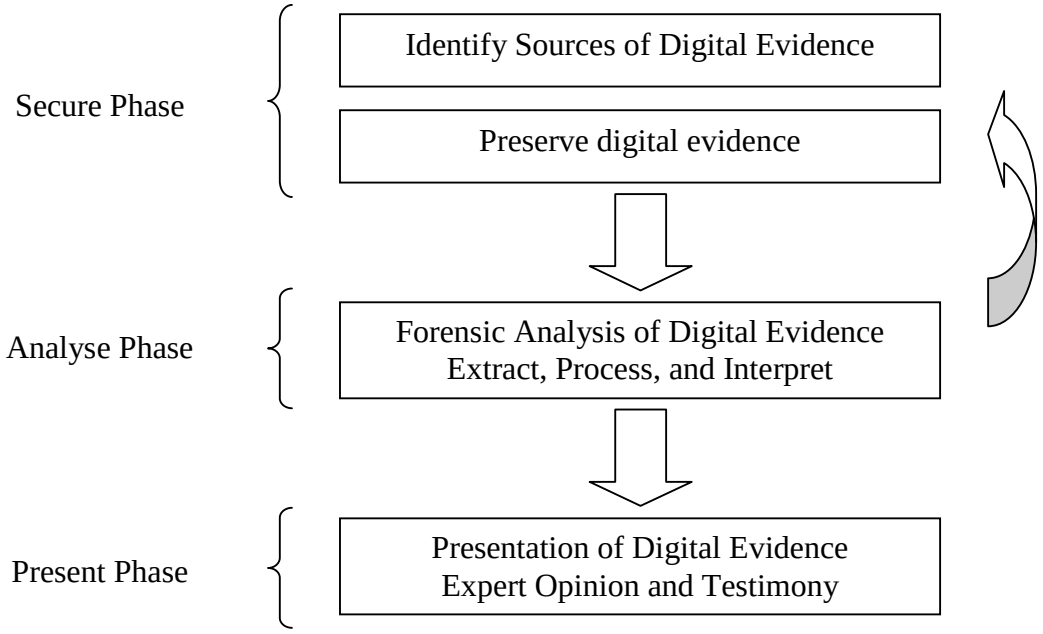


Figure 4: Concept of Computer Forensic – Secure, Analyse, Present Model

The CFSAP model can be considered an extension and refinement to McKemmish's earlier work from 1999. There are obvious parallels and similarities between these two works. The major differences between the CFSAP model and McKemmish's previous work are twofold. The first difference is that the phase called *Identification of Digital Evidence* and the phase called *Preservation of Digital Evidence* in McKemmish's work are merged into one phase called the *Secure* phase in the CFSAP model. This modification implies that the borderlines between the two original phases are sometimes not clear. This means that Mohay, Anderson, Collie, McKemmish and De Vel discovered that the two original phases are closely related to each other when the previous model was tested for four years.

The other manifest difference between the CFSAP model and McKemmish's previous work is that the concept of a flowchart is used to construct the CFSAP model. The addition of arrows shows the performing sequence of the CFSAP model. This modification gives the users a better understanding for the procedures of a computer

forensic investigation. Moreover, a retroactive arrow allows the movement from the *Analyse* phase to the *Secure* phase in the CFSAP model. The purpose of this recursive loop is to prevent overlooking of any possible digital evidence.

In summary, the CFSAP model shows that it is an upgraded version of McKemmish's previous work. The CFSAP model uses arrows to indicate the flow sequence of the procedures of a computer forensic investigation, and introduces a recursive loop to examine the relevant digital evidence more carefully. The idea of the recursive loop is similar to Enhanced Integrated Digital Investigation Process (EIDIP) model (Baryamureeba and Tushabe 2004) since the specific characteristic of EIDIP model is to allow computer forensic investigators to look back for any overlooked digital evidence. The EIDIP model is discussed below. The classifications used in the CFSAP model can be recognized as the best classifications in computer forensic field in Australia, since there is no similar academic research in the same direction.

Volonino (2003) gave a general process for the computer forensic investigation with only two main stages.

1. "*The discovery, recovery, preservation and control of electronic data or documents.*".
2. "*The analysis, verification and presentation of e-evidence in court or investigations.*".

The process proposed by Volonino has the same characteristic (generalization) as the other academic work cited here (Mckemmish (1999) in particular). In addition, combining the Volonino's practitioner model draws on work contained in two NIJ papers (National Institute of Justice 2001b; National Institute of Justice 2004) and shows how research-based computer forensic models are the foundation of practitioner-based computer forensic models. Thus, the relationship between Volonino's model and NIJ papers is an excellent verification of this concept.

Palmer (2001) proposed a research-based research model at the DFRWS. Whilst this model is unnamed, it will be referred to as the DFRWS model. The DFRWS model is comprised of six processes, with each process having some candidate methods or techniques. Table 1, which is drawn from Palmer (2001), shows every component of

DFRWS model. The top row of the Table 1 contains the six main processes. The column of each process shows the relevant techniques or methods that may be required.

Table 1: Digital Forensic Research Workshop Model

Identification	**Preservation**	**Collection**	**Examination**	**Analysis**	**Presentation**
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signature	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	Link	
		Data Reduction		Special	
		Recovery Techniques			

These techniques have been analysed in other work, with Stephenson (2003) referring to the definitions for the six processes in the 2003 DFRWS. According to Stephenson (2003), the definitions of Identification, Preservation, Collection, Examination, Analysis, and Presentation are listed below. Comparing Stephenson's work with McKemmish's work (McKemmish 1999), it is realized that Stephenson further expands the concept of preservation into preservation, collection, and examination phases. By doing this, Stephenson can provide more specific information for preserving digital evidence.

- Identification is defined as "*Determining items, components and data possible associated with the allegation or incident. Perhaps employing triage techniques*".
- Preservation is defined as "*Ensuring evidence integrity or state*".
- Collection is defined as "*Extracting or harvesting individual items or groupings*".
- Examination is defined as "*Closer scrutiny of items and their attributes (characteristics)*".
- Analysis is defined as "*Fusion, correlation and assimilation of material to for reasoned conclusions*".
- Presentation is defined as "*Reporting facts in an organized, clear, concise and objective manner*" (Stephenson 2003).

The issue raised by the DFRWS model is that it uses six general concepts to represent and to explain a whole computer forensic investigation. This is the typical feature of a research-based computer forensic model. Instead of providing explicit details for a computer forensic investigation, the DFRWS model shows the accurate direction for the relevant works. Moreover, DFRWS model has one particular characteristic, and this was described by Reith *et al* (2002) with the quote; "*The unique aspect of DFRWS model is that it is one of the first large-scale consortiums lead by academia rather that law enforcement*". This indicates that DFRWS model was not developed and created by one or two scholars, but it represents the consensus of many academic scholars. Thus, the DFRWS model plays a critical role in the field of computer forensics.

Reith *et al* (2002) not only described the unique characteristic of the DFRWS model, but also proposed a processing model called the Abstract Digital Forensics Model (ADFM). The ADFM consists of nine key components for a computer forensic investigation. The ADFM model is based on the DFRWS model, and therefore can be considered an extension of the DFRWS model.

The ADFM also draws from several other sources apart from the DFRWS model, such as the protocol for Federal Bureau of Investigation (FBI) crime scene search (Federal Bureau of Investigation 2003). Within the ADFM, the authors adopted nine stages to

represent a whole computer forensic investigation. The nine key components of the ADFM model are:

1. Identification - the purpose of identification is to identify the incident and to determine the type of the incident.
2. Preparation - the purpose of preparation is to organize necessary tools, required techniques, and search warrants.
3. Approach Strategy - the purpose of approach strategy is to dynamically build an approach. The goal of the approach not only can maximize the collection of the evidence, but also can minimize the impacts to the victim.
4. Preservation - the purpose of preservation is to protect and to maintain the current state of evidence. The evidence may include physical evidence and digital evidence.
5. Collection - the purpose of collection is to record the physical crime scene and to produce a duplicated image of digital evidence via qualified procedures.
6. Examination - the purpose of examination is to perform an advanced search for relevant evidence of the incident.
7. Analysis - the purpose of analysis is to provide an interpretation of the evidence, to construct the investigative hypothesis, and to offer the conclusions based on the found evidence.
8. Presentation - the purpose of presentation is to provide the explanations of conclusions.
9. Returning Evidence - the purpose of returning evidence is to make sure the physical and digital assets are returned to their owner

The ADFM has the following advantages and unique characteristics over other process models. First of all, the ADFM mentions the importance of preparation for a computer forensic investigation. The purpose of the preparation stage is to arrange for necessary tools, required techniques, and search warrants. These materials are important for a computer forensic investigation to proceed efficiently. The second advantage is based on the idea in the third stage of ADFM. The third stage describes the benefit of building an approach dynamically is helpful for a computer forensic investigation. These two considerations, especially the preparation stage, are usually lost in other research-based computer forensic models. However, according to Baryamureeba and Tushabe (2004), the problem with the ADFM is that the content of the *approach strategy* phase (the third

phase) is too close to the *preparation* phase (the second phase). Baryamureeba and Tushabe stated "*This is because at the time of responding to a notification of the incident, the identification of the appropriate procedure will likely entail the determination of techniques to be used.*".

In summary, the ADFM has exactly the same characteristics as other research-based computer forensic models. This indicates that the ADFM still have the problem of generalization. The ADFM proposes the preparation stage (the second stage) that is usually lost in other research-based computer forensic models. This stage is helpful for building practitioner-based computer forensic models, since a proper and prior preparation can avoid unnecessary disputes in the future. This is especially useful when performing a computer forensic investigation in reality.

Reith *et al* (2002) are not alone in adopting the concept of frameworks for physical crime scene search and adapting this for digital evidence. Carrier and Spafford (2003) proposed a model for a digital investigation, and the main concept of this model is based on theories and techniques derived from physical investigation models. This model is called the Integrated Digital Investigation Process (IDIP) model. The most well-known example of the physical investigation model can be found in the website of Federal Bureau of Investigation (Federal Bureau of Investigation 2003). The authors described their inspiration of their model, stating that "*The difference in activities between physical and digital forensics led the authors to the concept of a digital crime scene. Instead of treating the computer as a substance that needed to be identified, it is treated as a secondary crime scene. It should be treated as though the computer is a door that leads the investigations to a new room. When viewed in this way, the same principles that are used to process a room where jewellery was stolen can be used to process a server where credit card numbers were stolen – although the technology required to perform the process will obviously be different.*". They further wrote that "*A computer itself is, typically, only one piece of physical evidence, but it can be processed to identify thousands of pieces of digital evidence and each piece of digital evidence can be analysed to identify ownership, location, and timing. The digital evidence can be analysed to produce similar characteristics as physical evidence. Therefore, the investigation of billions of bytes of digital data is similar to the investigation of a house where an investigator must look at thousands of objects, fibers, and surface areas and use his experience to identify potential evidence that should be sent to a lab for*

analysis.". From the above two quotes, the IDIP model has two major features. The first of these features is that the IDIP model is built on existing systems for physical crime investigations. This infers that the reliability and credibility of the IDIP model are not an issue, as it is based on existing tested systems. In addition, the second characteristic of the IDIP model is that computers are treated from a different perspective. In the past, if a computer was found at a crime scene, it was considered physical evidence. This type of attitude places the role of a computer as exactly the same as a television or an air conditioner. However, with the growth of electronic crimes, they proposed a standpoint to observe the physical crime scene from a different angle. Carrier and Spafford (2003) described that the computer itself is no longer physical evidence, but the computer is a digital crime scene in a physical crime scene (e.g. private house or office). This perspective is especially important since the role of a computer in a crime scene is sometimes confused.

The IDIP model proposed by Carrier and Spafford (2003) contains five phases, which are further broken down into 17 sub-phases. These main phases and sub-phases are:

1. Readiness Phases

   The purpose of the readiness phases is to prepare necessary operations and infrastructure for a computer forensic investigation. It has two sub-phases.

   1.1 Operation Readiness Phase
   1.2 Infrastructure Readiness Phase

2. Deployment Phases

   The purpose of deployment phases is to offer a mechanism to detect and to authenticate the digital incidents.

   2.1 Detection and Notification Phase
   2.2 Confirmation and Authorization Phase

3. Physical Crime Scene Investigation Phases

   The purpose of physical crime scene investigation phases is to collect and to analyse any evidence which was left in the physical crime scene. In addition, the evidence must be occurred during the incident.

3.1 Preservation Phase

3.2 Survey Phase

3.3 Documentation Phase

3.4 Search and Collection Phase

3.5 Reconstruction Phase

3.6 Presentation Phase

4. Digital Crime Scene Investigation Phases

   The purpose of digital crime scene investigation phases is to collect and to analyse any digital evidence which was left in the physical crime scene. In addition, the digital evidence must be the evidence occurred during the incident.

   4.1 Presentation Phase

   4.2 Survey Phase

   4.3 Documentation Phase

   4.4 Search and Collection Phase

   4.5 Reconstruction Phase

   4.6 Presentation Phase

5. Review Phase

   The purpose of review phase is to provide a chance for investigators to re-evaluate the whole investigation by identifying areas of improvement.

Carrier and Spafford (2003) suggested that the preparation for a computer forensic investigation needs to be done before any further investigation proceeds. Therefore, the IDIP model contains a readiness phase as the first stage of the model. This means that the authors agreed the concept of ADFM model proposed by Reith *et al* (2002), since Reith *et al* put emphasis on the preparation stage of a computer forensic process as well.

In addition, Carrier and Spafford (2003) also adapted the third phase (*physical crime scene investigation* phase) and the forth phase (*digital crime scene investigation* phase) of the IDIP model to use similar concepts as the CFSAP model proposed by Mohay *et al* (2003). Within the physical crime scene investigation phase, there are six sub-phases. The interesting phenomenon occurs in the *survey* phase (phase 3.2), and *search and*

collection phase (phase 3.4). The purpose of *survey* phase is to identify the noticeable evidence left in the physical crime scene, and the meaning of *search and collection* phase is to perform an advance search to find out any possible evidence that is left behind. This means that if the *survey phase* and *search and collection phase* are considered as a whole, they act like a loop in the CFSAP model.

A similar situation occurs in the *digital crime scene investigation* phase of the IDIP model. For example, if a keyword is identified within the *survey* phase (phase 4.2), a further keyword search for any relevant digital evidence can be performed in *search and collection* phase (phase 4.4). This idea is again responding to the concept of the loop within the CFSAP model. The only difference is that the CFSAP model does not provide details to distinguish the physical evidence from the digital evidence. CFSAP model only focuses on the problems of digital evidence. From IDIP model and CFSAP model, it is realized that the latest trend of research-based computer forensic models is to allow computer forensic investigators to look back for any possible overlooking of the evidence.

In 2004, Baryamureeba and Tushabe (2004) proposed an extension to the IDIP model, titled *EIDIP model*. The EIDIP model is heavily based upon the IDIP model developed by Carrier and Spafford (2003), but adds some improvements. Some phases in the EIDIP model are derived from and directly comparable to the work of Carrier and Spafford (2003). However, the authors added two additional phases in the proposed EIDIP model. One is called the *Traceback Phase*, and the other is called the *Dynamite Phase*. The concept of the EIDIP model is to separate the investigation into primary crime scene (computer and its data) and secondary crime scene (physical crime scene). The ultimate goal of the EIDIP model is to build a reconstruction after all investigations rather than performing two reconstructions for primary crime scene and secondary crime scene. Building two reconstructions is the characteristic of IDIP model. The single reconstruction can prevent any possible inconsistent of two reconstructions.

Since the concept of the EIDIP model is derived from the IDIP model, the EIDIP model has similar advantages and disadvantages to the IDIP model. Here, the advantages and disadvantages of EIDIP are not discussed due to the similarities between the EIDIP model and the IDIP model. Besides the characteristics derived from the IDIP model, the EIDIP model has two major benefits. The first benefit is that the performance sequence

of the EIDIP model is iterative rather than linear. This is the unique feature of EIDIP model. The iterative performing sequence of EIDIP model means to perform every main phase in the EIDIP model is iterative. This concept can be seen in the Figure 5. A similar characteristic can be found in the CFSAP model and the IDIP model. However, only some phases in the CFSAP model and the IDIP model can work iteratively. In the CFSAP model, the recursive loop indicates the performing sequence can work from *secure* phase to *analyse* phase or from *analyse* phase to *secure* phase. Moreover, in the IDIP model, this recursive idea can be found within *physical crime scene investigation* phase and *digital crime scene investigation* phase. Unlike the IDIP model, the second benefit of the EIDIP model is that it only builds a single reconstruction after all investigations, including physical investigations and digital investigations. In IDIP model, two reconstructions are needed. One is for the physical crime scene, and the other is for the digital crime scene. This means that the EIDIP model can avoid any possible inconsistent between physical crime scene reconstruction and digital crime scene reconstruction.

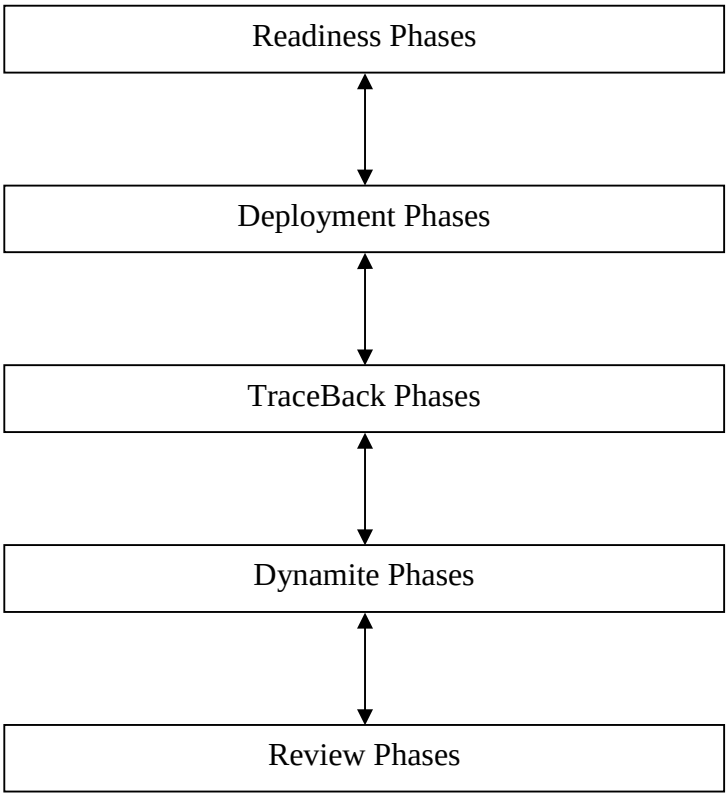


Figure 5: The Concept of Iterative Phases in Enhanced Integrated Digital Investigation Process Model

2.2.3.2 Practitioner-Based General Procedures of Computer Forensics

Before any further discussion of practitioner-based computer forensic models, a standpoint held in this thesis must be clarified. In this thesis, practitioner-based computer forensic models are considered to be derived from research-based computer forensic models. Due to the efforts done on research-based computer forensic models, the development of practitioner-based computer forensic models can then proceed smoothly and effortlessly.

In this section, general frameworks proposed by certain practical organizations are introduced. For example, *United States Department of Justice, National Institute of Justice* provides three outstanding papers within the field of computer forensics. These three papers are: *Electronic Crime Scene Investigation – A Guide for First Responders* (National Institute of Justice 2001b), *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (National Institute of Justice 2004), and *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (National Institute of Justice 2007).

Despite being written in 2001, National Institute of Justice (2001b) provides more comprehensive details compared with the research-based general models discussed in the previous section. Thus, this means that the work is more suitable for a practical application. In addition, National Institute of Justice (2004) can be considered the subsequent work with different focuses. In 2007, the latest paper (National Institute of Justice 2007) in this series puts emphasis on court related issues within the field of computer forensics.

The purpose of (National Institute of Justice 2001b) is to offer instructions for first responders. The responders may not necessarily be computer forensic investigators. They could be local or federal police officers. Thus, National Institute of Justice (2001b) only puts emphasis on *digital evidence collection phase* rather than *digital evidence examination phase*, *digital evidence analysis phase*, and *digital evidence reporting phase*. These four phases are mentioned in both National Institute of Justice (2001b) and National Institute of Justice (2004), and considered proper functions for a complete computer forensic investigation. The digital evidence collection phase is explained in National Institute of Justice (2001b), and the other three phases are

clarified in National Institute of Justice (2004). The relationship among both NIJ works and the four conceptual phases can be found in Figure 6.

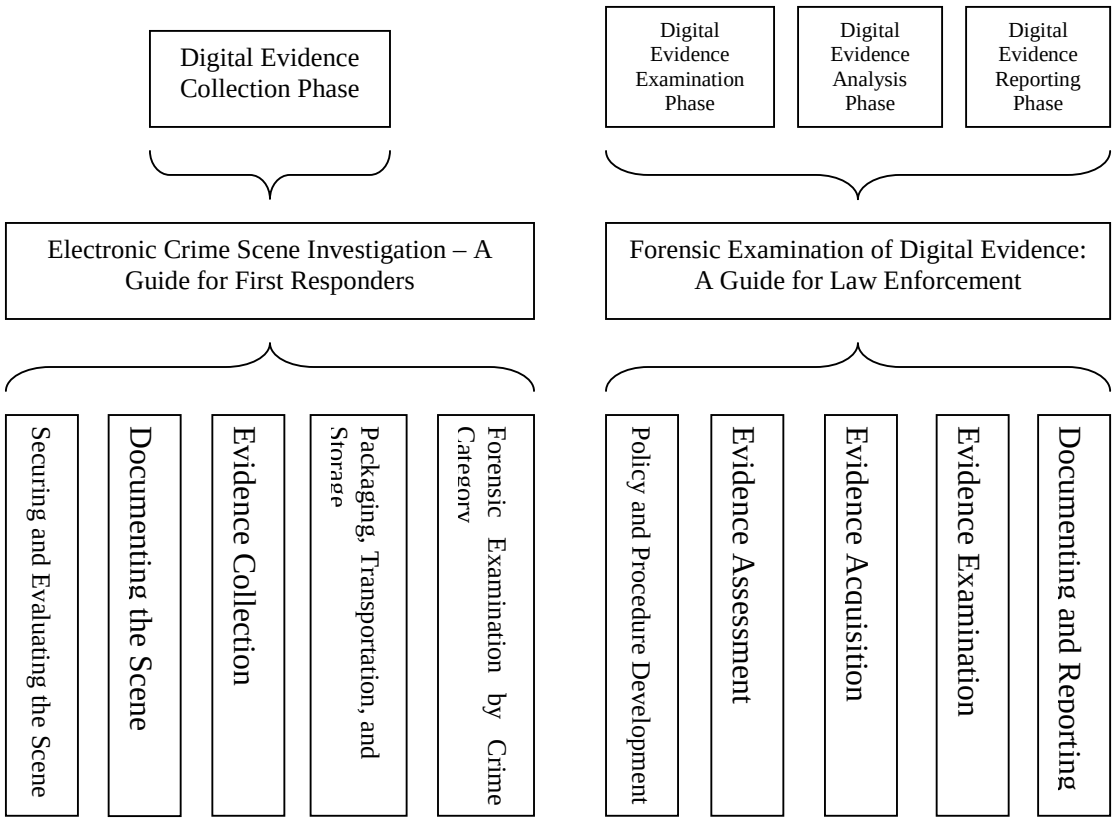


Figure 6: The Relationship among Electronic Crime Scene Investigation – A Guide for First Responders, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, and four conceptual phases

The major difference between research-based computer forensic works and practitioner-based computer forensic works is that research-based computer forensic works normally provide general commands and common concepts for computer forensic investigators. For example, National Institute of Justice (2001b) provides comprehensive details by presenting several exhaustive sub-phases of digital evidence collection phase, and these sub-phases are: *1. Securing and Evaluating the Scene, 2. Documenting the Scene, 3. Evidence Collection, 4. Packaging, Transportation, and Storage,* and *5. Forensic Examination by Crime Category*. By adopting these sub-phases, specific instructions can be provided rather than relying on the board and general phases. This gives computer forensic investigators concrete orders to follow. They then do not need to guess '*what the next step is?*' or '*if I do this, what should I do next?*'. The clear instructions are important and helpful because the digital evidence is eventually going

to be presented within a court. If the digital evidence is dealt wrongfully, it may become useless in a court and let the criminal walk out freely. The Figure 7 shows the structure of *Electronic Crime Scene Investigation – A Guide for First Responders* (National Institute of Justice 2001b), and the contents of five sub-phases are discussed below

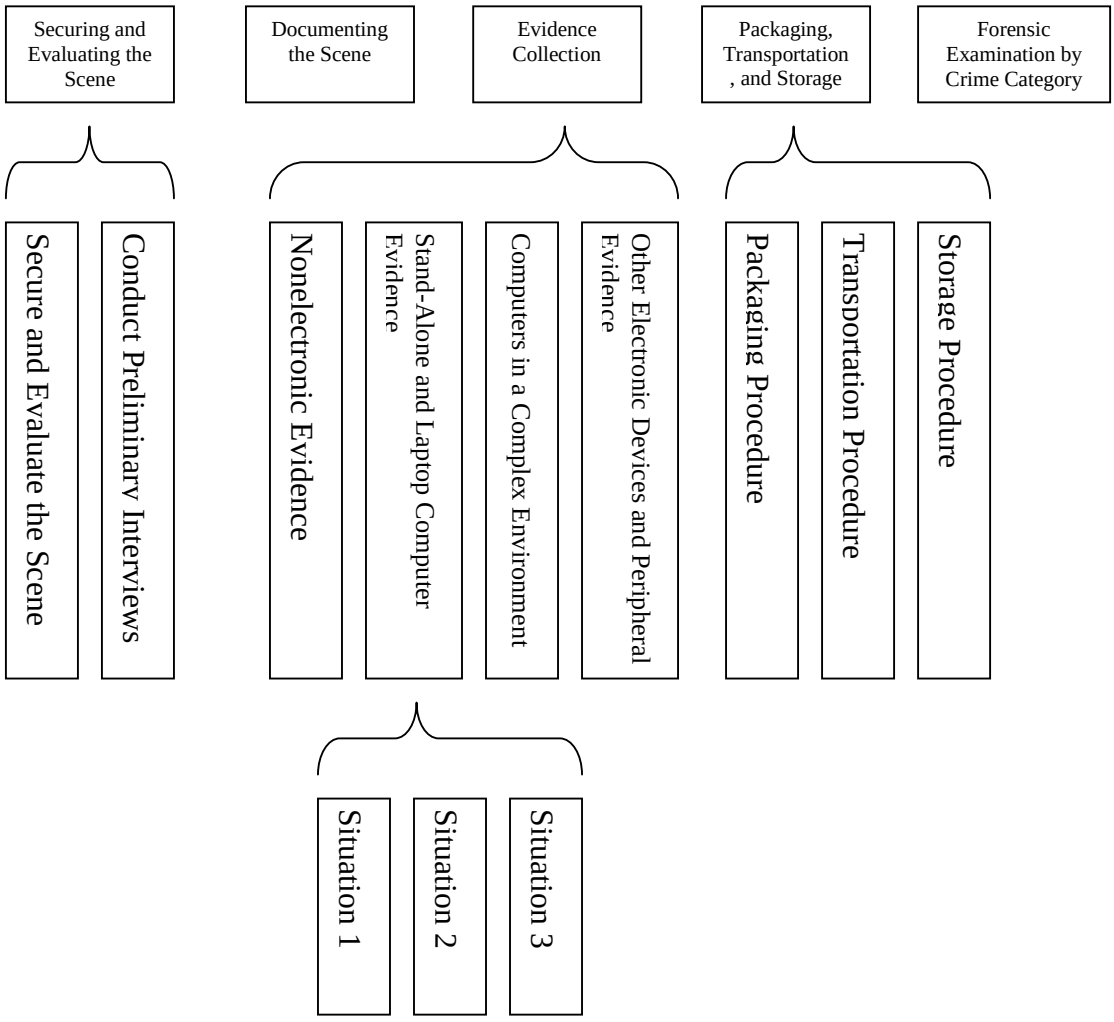


Figure 7: The Structure of Electronic Crime Scene Investigation – A Guide for First Responders

In the phase of securing and evaluating the scene, a core principle and procedure are provided. The principle is "*The first responder should take steps to ensure the safety of all persons at the scene and to protect the integrity of all evidence, both traditional and electronic.*", and the procedure is "*After securing the scene and all person on the scene, the first responder should visually identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. The first*

responder should evaluate the scene and formulate a search plan.". Besides a basic principle and an essential procedure, several thorough instructions are provided as well. For example, the primary rule for first responders at this phase is that they must not change the any electronic mechanism or device. This means that the first responders should maintain the situation of an electronic device once it is discovered. For example, if the electronic device is on, leave it on, or vice versa. In addition, the first responders should also determine that the fragile data should be immediately secured and documented. Lastly, people at crime scene are the responsibility of the first responders. The first responders must identify witnesses and document their positions.

From this point of view, it is realized that the responsibilities of first responders are very heavy and may be complex. They need to supervise the crime scene. Thus, it can be inferred that a computer forensic investigation is more complicated than just the collection of digital evidence, examining the digital evidence, or analysing the digital evidence. It needs cooperation of experts from different fields with diverse backgrounds.

In the phase of documenting the scene, the major principle and the major procedure are provided. The content of the principle is "*Documentation of the scene creates a permanent historical record of the scene. Documentation is an ongoing process throughout the investigation. It is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence.*", and the content of the procedure is "*The scene should be documented in detail.*". Besides the basic principle and the essential procedure, several thorough instructions are provide as well. For example, the first responders need to record the whole crime scene. This may include the locations of the computer, mouse, and keyboard, and the conditions of these equipments (e.g. power on, power off, or sleep mode) may also need to be chronicled. In addition, photographs are helpful for the future investigation or the future reconstruction in case the crime scene is contaminated.

In the phase of evidence collection, the principle is listed. The principle is "*Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation.*

Consideration should be given to protect data that may be susceptible to damage or alteration from electro-magnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.". In this action, four sub-aspects are offered so as to overcome the complex situation in the real world. The sub-aspects are: *Nonelectronic Evidence*, *Stand-Alone and Laptop Computer Evidence*, *Computers in a Complex Environment*, and *Other Electronic Devices and Peripheral Evidence*.

Nonelectronic evidence is sometimes very important in an electronic crime. For example, a password may be written on a piece of paper and be stuck to the computer. This means that it is possible for certain physical evidence to be very useful in an electronic crime investigation. Thus, first responders should not miss any type of evidence at the crime scene. Every relevant piece of evidence should be collected even it first looks irrelevant.

The definition of stand-alone computer is "*a computer not connected to a network or other computer.*" (National Institute of Justice 2001b). The author not only discussed stand-alone computer and a group of computers separately, but also gave further discussions for each category. In the area of stand-alone computer, three more procedures are listed, and each of them contains several sub-rules. However, none of the advanced procedures or sub-rules is debated in detail. The intention of this thesis is to show that National Institute of Justice (2001b) attempts to provide thorough solutions for a first responder. This is the typical characteristic of a practitioner-based computer forensic model.

Computers in a complex environment are another scenario proposed by National Institute of Justice (2001b). This situation occurs frequently in a business environment with more than one computer. Moreover, computers are likely networked with each other in this particular environment. This indicates any improper action may cause a damaging chain reaction. In this case, the damage is not limit to a single computer, but may affect other connected computers. The involvements of various operating systems can make this situation even worst. Therefore, the suggestion made in National Institute of Justice (2001b) is to seek professional help from experienced computer forensic investigators.

Other Electronic Devices and Peripheral Evidence is the last sub-aspect in the evidence collection. There are twenty six different types of devices listed in National Institute of Justice (2001b). This indicates that there are probably more types of devices when this thesis is written. In here, some uncommon devices are listed. They are copy machines, fax machines, pagers, PCMCIA cards, and telephones. Unlike computers and laptops, these uncommon devices are easily to be overlooked in the digital evidence menu.

In summary, collecting digital evidence is more complicated than just performing the action of *collecting*. According to the National Institute of Justice (2001b), digital evidence from different sources may need to be collected by different methods. This standpoint cannot be found in the research-based general models mentioned in the previous section. They merely mention a general concept but do not provide further features in detail.

For example, comparing National Institute of Justice (2001b) with the work proposed by McKemmish (1999), McKemmish's work provides four phases (identification of digital evidence, preservation of digital evidence, analysis of digital evidence, and presentation of digital evidence) to accomplish a computer forensic investigation. These four phases are the only elements for performing a computer forensic investigation in McKemmish's work. No sub-phase or further detail is mentioned. On the contrary, National Institute of Justice (2001b) has a complete opposite condition. Although it also suggests four phases (digital evidence collection phase, digital evidence examination phase, digital evidence analysis phase, and digital evidence reporting phase) for a computer forensic investigation, it attempts to cover every possible situations, and provides many details within these four phases. From this perspective, it is realized that the number of the phases in a model is not the only concern to decide its practicability. The details provided in each phase are the critical reason for this. Furthermore, comparing National Institute of Justice (2001b) with the research-based general models mentioned in the previous section, readers can find out that the evident characteristic and the leading benefit of National Institute of Justice (2001b) are that it not only provides details for each phase, but also concerns the situations of the crime scene from different angles.

In the phase of packaging, transportation, and storage, the principle is offered. The principle is "*Actions taken should not add, modify, or destroy data stored on a computer*

or other media. Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, and magnetic sources. Therefore, special precautions should be taken when packaging, transporting, and storing electronic evidence. To maintain chain of custody of electronic evidence, document its packaging, transportation, and storage.". The major concept of packaging is that the first responders must ensure every piece of digital evidence is well documented and labelled. The main concept of transportation is that the first responders must keep every piece of digital evidence away from magnetic and heat sources. The key concept of storage is that the first responders have to control the temperature and humidity of the store area.

It can be said that every computer forensic model contains a phase for maintaining the digital evidence. Normally the phase is called preservation phase. However, National Institute of Justice (2001b) again provides another aspect to deal the preservation issue. The concept of preservation phase is divided into three sub-concepts so as to give thorough explanations. This classification can be considered the unique characteristic of the model proposed in National Institute of Justice (2001b). Actually the concepts and the phases discussed in National Institute of Justice (2001b) are sometimes extremely common or mentioned in other works, but the new aspects are always used to interpret the ordinary concepts and phases. This is the contribution of National Institute of Justice (2001b).

In the phase of Forensic Examination by Crime Category, National Institute of Justice (2001b) provides the information for the first responders to match common file types to a specific crime category. Moreover, National Institute of Justice (2001b) lists a matrix for a computer forensic investigator to match the possible file types to a particular crime. None of the research-based general models mentioned in the previous section provides such matrix. In fact, there is no similar matrix existed. From this, readers can easily understand the value of National Institute of Justice (2001b).

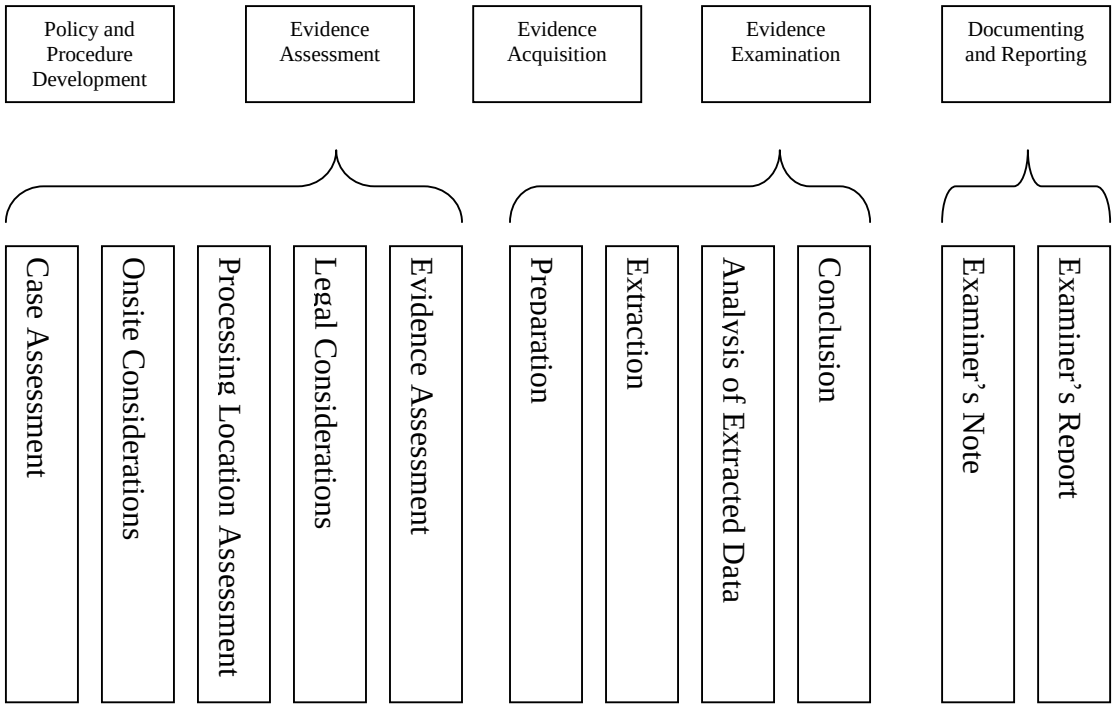


Figure 8: The Structure of Forensic Examination of Digital Evidence: A Guide for Law Enforcement

National Institute of Justice (2004) focuses on the concepts of digital evidence examination phase, digital evidence analysis phase and digital evidence reporting phase within a computer forensic investigation, and uses five sub-phases to further explain these concepts. The five sub-phases are: *Policy and Procedure Development*, *Evidence Assessment*, *Evidence Acquisition*, *Evidence Examination*, and *Documenting and Reporting*. The Figure 8 shows the structure of *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, and the detailed contents of these five sub-phases are discussed in the following paragraphs.

In the phase of Policy and Procedure Development, the major principle and the major procedure are provided. The content of the principle is "*Computer forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating. This can be attained by construction a comprehensive training program for examiners, sound digital evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency.*", and the content of the procedure is "*Departments should create policies and procedures for the establishment and/or operation of a computer forensics unit.*".

This phase mentions several important aspects within the field of computer forensics, which may include personnel training, personnel education, software license, and computer forensic policy. The major concern of this phase is similar to the preparation phase in the ADFM model, readiness phase in the IDIP model, and readiness phase in the EIDIP model. However, the only problem of National Institute of Justice (2004) is that the policy and procedure development phase should appear at beginning of any action of a computer forensic investigation. This means that the policy and procedure development phase should probably be displayed as chapter one in National Institute of Justice (2001b) rather than in National Institute of Justice (2004). The preparation phases is important than any other phases within a computer forensic investigation.

In the phase of Evidence Assessment, the major principle and the major procedure are provided. The content of the principle is "*The digital evidence should be thoroughly assessed with respect to the scope of the case to determine the course of action.*", and the content of the procedure is "*Conduct a thorough assessment by reviewing the search warrant or other legal authorization, case detail, nature of hardware and software, potential evidence sought, and the circumstances surrounding the acquisition of the evidence to be examined.*". Several sub-aspects are provided for computer forensic investigators to perform a thorough assessment. Comparing this concept with the concepts of research-based models, the action of the assessment is normally included in the examination phase or analysis phase in research-based computer forensic models due to different definitions. This is another explicit proof to demonstrate that the computer forensic process proposed in National Institute of Justice (2001b), and National Institute of Justice (2004) which provide more details than research-based works. These two papers sometimes consider a computer forensic investigation from different angles, and then occasionally provide brand new standpoints.

In the phase of Evidence Acquisition, the major principle and the major procedure are provided. The content of the principle is "*Digital evidence, by its very natural, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.*", and the content of the procedure is "*Acquire the original digital evidence in a manner that protects and preserves the evidence. The following bullets outline the basic steps.*". Evidence Acquisition phase can rarely be seen as an individual phase in research-based

computer forensic models. This is because the action of acquisition is normally included in the evidence identification phase or evidence collection phase depends on the different definitions.

In the phase of Evidence Examination, the major principle and the major procedure are provided. The content of the principle is "*General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination. Persons conducting an examination of digital evidence should be trained for this purpose.*", and the content of the procedure is "*Conduct the examination on data that have been acquired using accepted forensic procedures. Whenever possible, the examination should not be conducted on original evidence.*". The evidence examination phase can be considered the most technical phase in a computer forensic model. For example, a local police officer can secure the crime scene and collect the digital evidence very well, as long as the proper manual and corresponding instructions are given. However, it is almost impossible for a local police officer to examine the collected digital evidence without having official training programs or formal education courses. In addition, this phase can be found in both research-based computer forensic models and practitioner-based computer forensic models, since the digital evidence is not logical by its original format. People cannot understand the meaning of the binary digits unless a proper interpretation is made. In addition, this proper interpretation must not breach the integrity of the examined digital evidence. Based on the National Institute of Justice (2001b) and National Institute of Justice (2004), it is realized that a computer forensic investigation is comprised of several segments, and none of these segments can be treated careless. A tiny mistake in a segment may affect credibility of digital evidence in the later segments. In summary, the interpretations are necessary for mankind to understand binary digits, and are needed to be treated carefully and professionally. This phase is one out of few phases that every academic researcher and real world practitioner both agree.

In the phase of Documenting and Reporting, the major principle and the major procedure are provided. The content of the principle is "*The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.*", and the content of the procedure is "*All documentation should*

be complete, accurate, and comprehensive. The resulting report should be written for the intended audience.". The situation of documenting and reporting phase is the same as the evidence examination phase mentioned above. The concept of the documenting and reporting phase can be found in every proposed computer forensic model, including research-based and practitioner-based computer forensic models. There is no argument for this phase to be presented in the last step of a computer forensic model. This is because the examined digital evidence is eventually going to be used and presented in a court of law. Thus, a accurate, complete and understandable report is necessary for people without technical backgrounds, such as the judge, the lawyer, and the jury.

Although the procedures proposed in these two papers are not perfect (e.g. wireless forensics is not mentioned), one thing that cannot be denied is that these two papers provide a more precise view of a computer forensic investigation than other existed works. Moreover, if National Institute of Justice (2001b) and National Institute of Justice (2004) are considered jointly, the concepts proposed in these two papers can be treated as the expended works based on the concept proposed by Volonino (2003). Volonino (2003) offered a computer forensic model with two phases. The first phase is to discover, recover, preserve and control the electronic data or documents, and the second phase is to analyse, verify, and present the electronic evidence in a court.

Comparing National Institute of Justice (2001b) and National Institute of Justice (2004) with Volonino's work, it can be found that the concept discussed in National Institute of Justice (2001b) is close to the first phase of Volonino's work, and the three processing phases discussed in National Institute of Justice (2004) are analogous to the second phase of Volonino's work. In conclusion, the number of the phases within a computer forensic model is not the only concern to decide the value of the model. The only thing matter is that a computer forensic model must provide enough details so as to have a practical use.

The latest paper proposed by NIJ is *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (National Institute of Justice 2007) which discussed about the guidelines for law enforcement and prosecutors. Four main dimensions were proposed when presenting digital evidence in a court of law. This one points out the legal issues, such as different laws, validity of digital evidence, criteria for jury selection, and diplomacies with in a court of law, rather than giving a performing

sequence of a computer forensic investigation. Instead of collecting and analysing digital evidence, this paper focuses on discussions of legal issues. These four dimensions contain sub-issues, and they are listed below.

1. Search and Seizure Issues
   - 1.1 Background
   - 1.2 Wiretap Act
   - 1.3 Pen/Trap Statute
   - 1.4 Stored communications Provisions of Electronic Communications Privacy Act
   - 1.5 Privacy Protection Act
   - 1.6 Constitutional Issues
   - 1.7 Privileged or Proprietary Information
   - 1.8 Obtaining Out-of-State Recodes

2. Integrity, Discovery, and Disclosure of Digital Evidence
   - 2.1 Preliminary Inquiries
   - 2.2 Integrity of Data
   - 2.3 Building the Record to make the Case
   - 2.4 Returning Original Evidence
   - 2.5 Obligations to Disclose Evidence to the Defence

3. Courtroom Preparation and Evidence Rules
   - 3.1 Preliminary Considerations
   - 3.2 Pretrial Communication
   - 3.3 Evidentiary Considerations

4. Presentation of Digital Evidence
   - 4.1 Educating the Audience
   - 4.2 What Needs to be Proved or Disproved?
   - 4.3 Expert Witnesses and Technical Evidence
   - 4.4 Recurring Issues in Computer Crime Trials
   - 4.5 Jury selection
   - 4.6 Presenting Complicated and Technical Issues
   - 4.7 Closing Argument

The argument about ‘presenting digital evidence within a court of law is the ultimate goal of computer forensics’ is proved to be correct by the contents provided by National Institute of Justice (2007). The contents in this paper respond to the discussions in the Section 2.2.2.2. National Institute of Justice (2007) not only provided a concrete example about the usage of digital evidence in a court of law in reality, but also implicitly inferred the importance of the SOPs. Since presenting digital evidence is the ultimate goal of a computer forensic investigation, a proper and admitted procedure is important to make sure the validity, reliability, and credibility of digital evidence. Thus, the next section discusses SOPs issues within the field of computer forensics.

In conclusion, the concepts of the three NIJ papers (National Institute of Justice 2001b; National Institute of Justice 2004; National Institute of Justice 2007) are based on simple and well-known ideas within the computer forensic field, and then are built on with more consideration. These well-known ideas are collecting the digital evidence, analysing the digital evidence, and presenting the digital evidence. These basic ideas can be seen as the fundamental factors of all computer forensic models. Moreover, if the three NIJ papers are considered as a whole, they can be seen as one of the most pragmatic computer forensic models in the world at this moment.

Besides the three NIJ papers, ACPO and Scientific Working Group on Digital Evidence (SWGDE) are two other formal agencies, belonging to Great Britain and the United States of America respectively, who provide official reports on computer forensic procedures as well. For example, the Good Practice Guide for Computer based Electronic Evidence (Association of Chief Police Officers 2003), SWGDE recommended Guidelines for Validation Testing (Scientific Working Group on Digital Evidence 2004a)**,** Developing Standard Operating Procedures (Scientific Working Group on Digital Evidence 2004b), Best Practices for Computer Forensics (Scientific Working Group on Digital Evidence 2005), and Best Practices for Computer Forensics (Scientific Working Group on Digital Evidence 2006).

It is thus accepted that there are many practitioner-based computer forensic models in existence and these are built on differing research- based models. Since the purpose of this thesis is to focus on the impact of culture on Australian and Taiwanese computer forensic procedures then several relevant questions, drawing on the above section of the

literature review are asked in the Delphi questionnaire, in order to determine any possible cultural differences in forensic models between Australia and Taiwan.

2.2.3.3 Standard Operating Procedure of Computer Forensics

A SOPs can be seen as the ultimate goal of the practitioner-based computer forensic models. According to the discussions of research-based computer forensic models and practitioner-based computer forensic models, procedures for performing computer forensics have obtained attentions for several years. Proper procedures are essential for computer forensic practitioners to perform a computer forensic investigation correctly, and to ensure the validity, legitimacy, and reliability of digital evidence (Pollitt 1995b; Civie and Civie 1998; Lin *et al* 2003a; Lin *et al* 2003b; Lin *et al* 2005). An example is given to show the importance of having SOPs.

Due to the lack of SOPs, investigator A is allowed to use method A to collect the digital evidence, and investigator B, on the other hand, is able to use method B to collect the digital evidence as well. In this situation, there is no standard to judge the correctness of method A and method B. Method A may be considered an acceptable way to collect the evidence, but it may also have the possibility of being attacked by the defendant's attorney as an improper method. Moreover, this situation is very likely to occur when the unqualified method B is used. In this manner, there is no guarantee of the quality of the digital evidence without a proper and admitted procedure.

Definitions of SOPs have been discussed for several years. For example, Pollitt (1995b) noted "*Standards serve as a guarantee, to those not involved, of reliable results. Standards serve to limit liability for actions by the examiner and his organization. Courts have been more willing to accept scientific evidence where there have been standards by the pertinent scientific community. It is a matter of time before standards for forensic examination will be demanded.*". Lin *et al* (2003b) stated that "*In order to provide the appropriate assistance for prosecutor, police, investigator in the process of the case, it must create a SOP and a common procedure of warrant search of Cyber Security, therefore, the law enforcement in the event may process the case by SOP. Thus all the procedures in the issues of searching, discovery, retrieving, preserving, transportation and forensic of the digital evidence should be distinctly regulated and stipulated by the law. It's to provide the rule of execution for all the personnel within*

the investigation and Cyber Security Forensic". In addition, Lin *et al* (2003a) repeated this argument. The above arguments point out that a SOP for computer forensics is demanded due to the legal purposes of digital evidence. Pollitt (1995b) interpreted the issues of SOPs from scientific perspective, and Lin *et al* (2003b) focused more on the legal consequences which are caused by an improper set of computer forensic SOPs.

In addition, Pollitt (1995b), Lin *et al* (2003a), and Lin *et al* (2003b), Meyers and Rogers (2004) all agreed that the significance of a set of SOPs in the computer forensic field is profound, and stated that SOPs must have flexibility in order to allow for revisions since the world of computer forensics changes continuously and rapidly. A permanent set of SOPs is likely to become impractical and valueless. Pollitt (1995b) stated that "*Standards can serve to impede progress and limit creativity. As new problems and new tools become available, new methods of solving forensic problems will be created. Although most physical sciences are evolving, their basic, underlying basis is not changing. Certainly not with the vigour that has been that hallmark of the computer industry. Unless care is taken to build in flexibility, any computer related standards are doomed to failure.*". This implies that building SOPs is a continuous job. Regular updates and routine checks of the SOPs are necessary as so to overcome the changing situations. Permanent SOPs may eventually become useless and outdated.

The ultimate aim for computer forensic practitioners is to build a unified set of SOPs. However, this lack of SOPs is expanded upon by Palmer (2001) with the statement "*Analytical procedures and protocols are not standardized nor do practitioners and researcher uses standard terminology.*". In additional, Reith *et al* (2002) said similar contention, "*In many crimes, the procedures for accomplishing forensics are neither consistent nor standardized.*", to describe the current SOP situation within the field of computer forensics. The lack of a set of SOPs in the field of computer forensics is understandable for several reasons: 1. every case is slightly different, 2. rapidly changing technology, and 3. legislative issues require extensive customisation. The first reason, that the case under determination is sometimes unique is a potential issue as a SOP is not likely to be entirely applicable to every circumstance, unless it is highly complex. The second reason is that the technologies not only change continually, but also change rapidly. Therefore, a high quality set of SOPs today may become outdated tomorrow due to new technologies and new digital devices. From this point of view, a fixed set of SOPs for computer forensics is very likely to become a barrier for any

possible further development. The third reason is that a set of SOPs may be suitable for an individual legislation but inappropriate for others. Different legislations may alter the acceptance of digital evidence or procedures, and what is acceptable in one jurisdiction may not be in another. Therefore, a set of SOPs would need to be independently developed for each legislative boundary. For example, Australian common law has different regulations from Taiwanese civil law. Discovery (Christopher and Hidgekiss 2006; Davies 2006) is an evident example. The purpose of discovery is to require the plaintiff and the corresponding defendant to exchange any relevant evidence of the case. There is no such concept in Taiwanese civil law. This indicates that SOPs, if they existed, for Australian computer forensic investigators may not work for Taiwanese computer forensic investigators, and vice versa. The through discussions of discovery can be found in the Section 2.2.4.3.

As can be deduced from the previous discussion a set of SOPs is a topical issue in the computer forensic field, and academic scholars have already discussed this issue for several years. The necessity of a set of SOPs is a necessity for the purpose of computer forensics since SOPs can ensure the quality, the validity, and the reliability of digital evidence (Pollitt 1995b; Lin *et al* 2003b). This is helpful when presenting the digital evidence in a court. It is essential for computer forensic researchers or investigators to leave space for any possible future development of a set of flexible and more universal SOPs. This can prevent SOPs from becoming outdated and irrelevant, and can ensure the set of SOPs is adaptable. This indicates routine updates and regularly checks of SOPs may be required.

2.2.4 Current Issues of Computer Forensics

Unlike physics and/or chemistry, computer forensics is a young research subject within the field of science. New knowledge constantly needed to be discovered, and relevant research is ongoing in several important areas which are all relevant to computer forensic practice.

2.2.4.1 Certification of Computer Forensics

Meyers and Rogers (2004) have noted and criticised the lack of a professional certification in the field of computer forensics. They noted "*In order for the field of*

computer forensics to mature, there must be a national system for certifying individuals who claim to be professionals. The continued lack of a professional certification, investigative standards, and peer reviewed method, may ultimately result in computer forensics being relegated to a "junk science" as opposed to a recognized scientific discipline.". Meyers and Rogers are not alone in proposing this idea. This argument is also agreed with by Jones (2004). However, Jones (2004) used another avenue to describe the importance of certifications within the field of computer forensics. Jones (2004) discussed the issues of computer forensic certification by asking '*who are the experts?*' rather than focusing on computer forensic certifications directly and explicitly.

The standpoint proposed by Meyers and Rogers (2004) and Jones (2004) is further expanded and discussed in this section. This thesis discusses several dilemmas which may be caused by the issues of the lack of computer forensic certification. They are validity of digital evidence, validity of computer forensic experts, and the validity of the computer forensics itself.

Without proper certifications, the validity of digital evidence is very likely to become a problem in a court of law. It is very challenging for a lawyer to defend a case without knowing the trustworthiness of the digital evidence. Due to the same reason, a judge will find it very difficult to decide the result of a case based on questionable digital evidence.

In addition, how can an investigator claim himself/herself to be a computer forensic expert without proper accepted certifications? Under certain circumstances, it is straightforward for the defendant's lawyer to attack this flaw (qualifications of experts). As long as the lawyer challenges the validity of the computer forensic expert, all collected digital evidence may be at risk.

Moreover, the validity of computer forensics is deeply affected by the lack of certifications and/or standards within computer forensics. If a certification and/or standards regime cannot be properly constructed, the validity of electronic evidence within computer forensics will eventually become a serious problem because the ultimate object of computer forensics is to present valid digital evidence within a court of law.

2.2.4.2 Encryption in Computer Forensics

Encryption applications are designed for legitimate purposes (e.g. security purpose, and privacy purpose). However, malicious users adopt this technique for nefarious purposes (e.g. terrorism) (Freeh 1997). The issues associated with encryption potentially causes challenges for law enforcement. Denning and Baugh (1997) stated that "*We then discuss the threat posed by encryption to law enforcement, public safety, and national security. The threat is manifest in four ways: failure to get evidence needed for convictions, failure to get intelligence vital to criminal investigations, failure to avert catastrophic or harmful attacks, and failure to get foreign intelligence vital to national security. Encryption can also delay investigations, increase their costs, and necessitate the use of investigative methods which are more dangerous or invasive of privacy.*". According to the same article, they gave a phenomenal statistic (given this article is ten years old and given the exponential growth in electronic crime and terrorism) to describe the increasing rate of criminal cases using encryption technique. They asserted "*Our findings suggest that the total number of criminal cases involving encryption world-wide is at least 500, with an annual growth rate of 50-100%.*".

In summary, the concept of encryption applications is a brilliant technique with both advantages and disadvantages. It is useful for protecting privacy and enhancing security but, if this technique is used by the wrong people for the wrong purposes, the results are catastrophic.

Above statements show the influences of encryption within a computer forensic investigation. More literature (Casey 2002; Wolfe 2004; Siegfried *et al* 2004) supported this argument, and they further proposed several possible approaches to overcome the obstacles caused by the use encryption techniques by suspects and criminals. These approaches are:

- **Social Engineering**

  Social engineering normally refers to malicious people take advantages of humanity weaknesses to achieve their malevolent purposes. Conversely, if computer forensic investigators use this technique properly, they may have the chance to obtain desirable information (e.g. password or decryption key) rather than using technical skills to find the weaknesses of the encryption algorithm or breaking the encryption algorithm by brute force attacks. In the field of social

engineering, a suspect's personal and/or private information is one of the valuable sources to help computer forensic investigators to obtain the wanted data (e.g. password or decryption key). The information may include: suspect's birthday, the birthday of his/her son/daughter, number plate of the car, mobile phone number, address of the house, name of the family pet, personal identification card, name of the favorite sport star, anniversary of marriage, and other data which is related to suspect's personality.

In short, the utility of social engineering shows that a simple method sometimes is very effective. The other good news for computer forensic investigators is that people often use words, which are related to them or important to them, to create the password. This indicates that it is likely for computer forensic investigators to be able to obtain hidden information without actually breaking the encryption algorithm.

- **Locating Unencrypted Copies**

  Before the data is encrypted, the plaintext may exist in somewhere of the computer. As stated by Casey (2002), "*while a file is being encrypted using Encrypting File System a temporary copy of the plaintext is made in case a problem is encountered during the encryption process.*". Another possibility is that plaintext may be momentarily stored in a paging file or on a disk. Moreover, Random Access Memory is another possible source to search for the plaintext.

  In summary, to search for an unencrypted copy is an intelligent method to side-step the challenges of encryption applications (e.g. brute force attack). Breaking the encryption algorithms is not the only choice for computer forensic investigators.

- **Obtaining Encryption Password**

  Obtaining encryption password is no doubt the most useful way to decrypt the encrypted data. However, this is also the biggest challenge for computer forensic investigators to solve. Several possible solutions are provided. For instance, computer forensic investigators can interview the suspect and try to convince the suspect to release the password. Another example is that computer forensic investigators can search for suspicious notes around the suspect's computer for

possible password. Furthermore, if it is available, using suspect's passwords for other purposes (e.g. e-mail protection, and bank account protection) is a good idea, since people normally use the same password for various purposes.

Based on the previous discussions, retrieving the correct password is not an impossible mission. It needs special skills and some luck.

- **Guessing Encryption Password**

  It is almost unfeasible for computer forensic investigators to guess suspect's password randomly. For example, 4 digit password may contain 1679616 (36^4) different combinations if Arabic numeral and English alphabet are used. Not mention more combinations for 6 digitals password or a password with more digitals. However, if computer forensic investigators are able to guess comparatively '*correctly*', it is still likely for them to retrieve the accurate password. In this paragraph, '*correct guess*' means using suspect's birthday, number plate of the car, mobile phone number, anniversary of marriage, or any personal affair to decide the estimated password.

  Concisely, guessing for the correct password is not an insurmountable task. Guessing with skill rather than guessing randomly is important, and sometimes fortune is necessary.

2.2.4.3 Electronic Discovery

In order to understand electronic discovery, the concept of discovery must be introduced first. In Australian common law, discovery (Christopher and Hidgekiss 2006; Davies 2006) is the pre-trial phase in a lawsuit in which each party through the civil procedures can request documents and other evidence from the other party, or can compel the production of evidence by using a subpoena or through other discovery devices, such as requests for production and depositions. Luoma (2006) provide the definition of discovery as "*The discovery process is the legal procedure used by parties to a lawsuit to obtain information from the opponent and other witnesses before the trial. The purpose of the discovery is to help a litigant to find the other litigant's version of the facts, what witnesses know, and other evidence that may exist.*". Using discovery can ensure that no party is going to be surprised by new evidence proposed by opponent at

the trial. Furthermore, using discovery also encourages a settlement before the trial since both parties fully understand about all relevant documents of each other.

With the popularity of electronic equipments (e.g. desktop, laptop, mobile phone, personal digital assistant, and digital camera), brand new terms are created, such as digital data, and digital evidence. As a consequence, digital evidence is well accepted by the public due to the massive usage of digital information. Electronic discovery is then created and used to deal with digitalized files. In fact, discovery can be considered the derivation of electronic discovery. This shows that the purpose of electronic discovery is also to ask the plaintiff and the corresponding respondent to exchange relevant digital evidence in a civil lawsuit, as long as the evidence is correlative to the case. Therefore, from a broader viewpoint, two conclusions can be made. The first conclusion is that electronic discovery and discovery are essentially the same. The major difference between them is that they deal with different types of evidence. The second conclusion is that to perform electronic discovery involves the techniques of computer forensics due to the involvement of digital evidence.

Since performing electronic discovery requires unique and special techniques within computer forensics, the problems encountered by electronic discovery are actually the problems which are needed to be confronted in the field of computer forensics. This thesis lists some general characteristics of electronic discovery, and they are:

1. Since electronic discovery usually process digital data, important meta-data may be generated when the original data be accessed. The meta-data may contain 1) who accessed the data, 2) when the data be accessed, 3) when the data be printed, and 4) when the data be modified. These types of information are almost impossible to be discovered in paper-based documents.

2. It is very easy to duplicate the digital data. One original data may have multiple copies and they are stored in different places. Hence quantity of copies becomes an issue in electronic discovery.

3. Lawyers, plaintiffs or defendants may not have enough technical skill to perform electronic discovery. Therefore, well-trained experts may be required to discover the related data.

4. Special hardware or software may be needed to discover the data. For example, retrieving deleted data needs particular software/hardware is not a surprise.

5. It can be said that the electronic discovery is more complex and more expensive exercise than traditional discovery. Therefore, it is almost impossible to avoid the additional costs for electronic discovery.

6. The privacy of participants and the confidentiality of documents have higher possibilities to be violated. Therefore the electronic discovery must be undertaken under the protection of the legal procedures.

In addition, some following problems which may occur by performing electronic discovery are listed below.

1. How to prove the authority of digital evidence? Irrelevant digital document cannot become the useful evidence.

2. How to find the relationship between relevant documents? All related data to an original copy need to be discovered.

3. How to retrieve valuable information without damaging the origin copy? To retrieve a document is more than just copying the original copy. It usually needs particular computer forensic software/hardware.

4. Is IT department capable of dealing with this type of work? Since a company already hired people for IT department, a company normally depends on them to fix any type of computer related problems, but the question is '*Can they do this job properly?*'.

5. Is it necessary to hire experts to do this work? If the answer is '*yes*', additional costs are needed for hiring the forensic experts. It is sometimes hard to understand for a company that spending money only for preparing the trial before the start of the real trial. If the answer is '*no*', the problem is changed to '*Who is going to do this job?*'.

6. Does the retrieving information admissible in a court? If the data are processed by a person who is not entitled in a wrong way, a court may refuse to accept them as evidence.

2.2.5 Is Computer Forensics Science?

The answer of '*Is computer forensics science?*' is undoubtedly '*yes*'. The thorough reasons are given as follows. There are numerous studies about forensic science (often shortened to forensics) (Robertson and Vignaux 1995; Ramsland 2001; Saferstein 2001; Platt 2006; Crispino 2007). This apparently shows that forensics itself is a science. Although the term '*forensics*' normally refers to DNA testing, fingerprint testing, drug testing, and blood testing, it cannot be denied that computer forensics is a branch of forensic science. This infers that computer forensics is a subject of science. Two demonstrations are provided, and they indeed echo this standpoint

Volonino *et al* (2007) stated that "*In the United States, courts at many levels and in many jurisdictions have recognized computer forensics as a bona fide scientific method of discovering and proving facts that can be used to solve and prosecute crimes. Recently, the forensic discipline of acquiring, preserving, retrieving, and presenting electronic data has been called* ***computer forensics science****. The new emphasis on this field as a science is important because it shows that computer forensics is a discipline based on generally accepted scientific methods. This recognition helps reinforce the credibility and stature of computer forensics investigators.*". It is straightforward to understand the meaning of this reference. It simply shows that the field of computer forensics is contained by the science. This statement is not questionable, since the first three authors (Volonino, anzalduam, and Godwin) of this book have Certified Information Systems Security Professional (CISSP) qualification.

Moreover, Kruse and Heiser (2002) stated that "*Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. It is often more of an art than a* ***science****, but as in any discipline, computer forensics specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual.*". Although Kruse and Heiser think computer forensics is more of an art than a science, they still admitted that computer forensics itself is science.

2.2.6 Summary of Section 2.2

Section 2.2 introduces the fundamental issues within computer forensics. In Section 2.2.2, computer forensic issues, such as the definition and the purpose of computer forensics are discussed, as well as the issues associated with digital evidence, such as the definition and the characteristic of digital evidence.

Section 2.2.3 focuses on the issues of procedures of computer forensic. Research-based and practitioner-based general procedures of computer forensics are shown and discussed. In addition, the issue of Standard Operating Procedures within computer forensics is discussed as well.

In Section 2.2.4, common obstacles within computer forensics are discussed as well. For example, the certification of computer forensics and the decryption issue are two major barriers within the field of computer forensics. Lastly, Section 2.2.5 confirms that computer forensics is a branch of science.

In summary, Section 2.2 shows some of the essential understanding of computer forensics, and provides a range of technical and scientific issues that might be considered universal and international within forensic computing investigations. These issues thus provide the foundation for a series of survey questions, for both Delphi expert group and case study as we move on to explore the research question and consider the impact of culture on computer forensics.

2.3 Culture

2.3.1 Overview of this Section

The purpose of this section is to review academic literature which examines the effect of culture on science and its applications, and the relation ship between culture and the study of Information Systems, Engineering and Computers in general.

A review of IS and CS research over the last few years shows an increasing interest in the role that culture plays in the design and engineering of complex ICT systems. Examples of research questions, alluded to in Chapter 1 include those contextualised within:

- Organisational and national culture, software specification and requirements analysis (Finkelstein and Fuks 1989)
- Culture and interface design (Cagiltay 1999)
- Cohesiveness of distributed teams working in a technologically mediated manner across national boundaries (Rathod and Miranda 1999; Vogel *et al* 2001)
- Cultural differences in virtual software teams (Dafoulas and Macaulay 2001)
- Cross-cultural perspectives within military ICT development (CCRP 2001)

This thesis extends, what discussed by (Straub *et al* 2002) in Chapter 1, then to see how our ability to develop theories and models for computer forensics is affected by our understanding of culture. In Section 2.3.2, definitions of culture are introduced. This is necessary since the understanding of culture is the essential prerequisite of this thesis. The most well-known and well-accepted cultural definition, provided by Geertz (1973), is chosen.

In Section 2.3.3, the relationship between culture and science applications, such as. science education, is introduced. This relationship is especially important since it shows that applications of science are affected by different cultures. Thus, the link between culture and science application is then established.

Finally, in Section 2.3.4, the work in Culture and IS is presented at length with a view to applying this in computer forensics.

2.3.2 Definition of Culture

Many different definitions of culture are found in literature ranging from anthropology, philosophy, teleology through to information system research. A fundamental understanding of culture is given by Geertz (1973) as "*Man is an animal suspended in webs of significance he himself has spun. I take culture to be those webs and the analysis of it is not an experimental science in search of law but an interpretative one in search of meaning.*". In this definition, Geertz stated that the meaning of culture is an interpretative concept, and culture is another way to express the social and cognitive development of an individual.

According to Soares *et al* (2007), Tylor, the early British anthropologist, defined culture in 1871 as "*the complex whole which includes knowledge, belief, art, morals, law, custom and any other capabilities and habits acquired by man as a member of society.*". This statement clearly shows that culture is a multi-disciplinary concept rather than a simple idea. In addition, Soares *et al* (2007) also stated that this definition of culture is one of the earliest descriptions and one on which many other researchers lean or draw meaning.

Hofstede (1980) defined culture as "*the collective mental programming of the people in an environment. Culture is not a characteristic of individuals; it encompasses a number of people who were conditioned by the same education and life experience.*". Hofstede (1989) refined the definition of culture from another perspective as "*The collective programming of the mind which distinguishes the members of one category of people from another. 'The category of people' can be a corporation but also a nation, an ethnic group, a profession, a type of business or industry, a generation or a work group.*". From Hofstede's definition of culture, it can be clearly understood that Western minds think differently from eastern minds. In addition, Hofstede's definition of culture was further interpreted by Shore and Cross (2005), they stated the understanding of culture as "*Culture can be defined as the set of mental programs, established early in life and difficult to change, that control or influence an individual's responses in a given context.*".

After presenting the diverse definitions of culture, it can be seen that culture is not a simple issue to define or to discuss. Culture can be considered a dynamic phenomenon rather than a static characteristic. Therefore, if people from different perspectives observe culture, they are very likely to provide varied responses. The cultural definition used in this thesis is the one proposed by Geertz (1973). This is because Geertz's cultural definition is the one accepted by scientists as well as anthropologists (Cobern 1991; Waldrip and Taylor 1995).

2.3.3 Culture and Science

After discussing the meaning of culture in Section 2.3.2, the link between culture and science must be built since a purpose of this thesis is to build on the fact that science is affected by culture. In order to do this, a question, *is culture universal?*, should be asked

so as to clarify the core concept of this thesis. If the answer of this question is '*no*', the link between different cultures and science then needs to be found and established. In the following paragraphs, several academic opinions (Vygotsky 1978; Wertsch 1985; Wertsch *et al* 1995; Solano-Flores and Nelson-Barber 2001; Greenfield 1997) are presented to defend this hypothesis.

The researchers above (Vygotsky 1978; Wertsch 1985; Wertsch *et al* 1995; Solano-Flores and Nelson-Barber 2001; Greenfield 1997) show that culture is not universal, and culture has the ability to affect an individual's mind and thinking. In addition, the authors also indicate that culture changes the way that an individual constructs knowledge, and forms experience.

Vygotsky (1978), Wertsch (1985), and Wertsch *et al* (1995) had similar thoughts. They all acknowledged that culture and society are two major factors which influence cognitive development. People with different cultural backgrounds are likely to act or to respond to an event differently. In addition, Solano-Flores and Nelson-Barber (2001) made a similar statement as "*The conceptual relevance of cultural validity is supported by evidence that culture and society shape an individual's mind and thinking.*". Lastly, Greenfield (1997) stated that the way for an individual to construct knowledge and create meaning from experience is affected by culture. The way that an individual thinks about things, and how he or she solves problems is affected by culture.

The aforementioned explanations and descriptions show that considerable academic literature answers the question, *is culture universal?*, in the negative. If it is agreed that different cultures influences the construction of knowledge and forming cognitive development (Hofstede 1986; Hofstede 1989; Hofstede 1993; Hofstede 1994), people from different countries have been shown to think differently.

This assumption is further discussed by Slay (2000b). In her PhD thesis, a statement was given as "*Within Western society, the cultural and historical differences which exist between China and the West are often acknowledged implicitly without being defined and articulated. An explanation for this might be that over the last few centuries, large parts of Africa, America, Asia, and Australasia have been fought over and colonised to a greater or lesser extent. From these 'power' relationships, a great deal of cultural familiarity has developed. However, a wide gap in cross-cultural understanding still*

exists between those shaped by their Western scientific world view and the Chinese who have lived and flourished with alternative traditions and perspectives since Stone Age times.". This statement shows that the cultural differences indeed exist between China and the West, and proves that culture is not a universal concept.

According to Cobern *et al* (1999), "*Worldview research in science education dates at least to Kilbourn (1984) and Proper, Wideen, and Ivany (1988). Cobern (1991) borrowed a logico-structural model of worldview from anthropologist Kearney (1984) in an attempt to bring greater coherence and sophistication to worldview research in science education.*". In addition, Cobern *et al* (1999) stated that "*Indeed, the criticism of modern Western scientific views of Nature (e.g. Merchant 1989) provides reason to investigate the views fostered in a science class. This line of thought suggests a broad agenda for cultural studies research in science education, premised on the assertion that all ideas, including scientific ones, are expressed within a cultural setting (Geertz 1973). Thus, one must ask how the cultural setting of the science teacher and curriculum compares with student cultural settings.*". From these two accounts, two conclusions can be made. The first conclusion is that the worldview research in science education is also research into culture and science education. The second conclusion is that the statements show that the research, worldview (culture) and science education, has existed for more than 20 years, and many scholars now devote themselves to this area.

Theocharis and Psimopoules (1987), Holton (1993), and Levitt and Gross (1994) all considered the issue of the effect of worldview differences on scientists' attentions to antiscientific views. This means that worldview differences are indirectly shaping an individual's views of science, and also implicitly echoes the fact that the culture is not universal, and that culture has influence on science.

Ogawa (1998) expressed the view that science and science education can be considered the expression of the understanding by the people of that culture, and this situation is applicable in any culture. What is expressed by Ogawa is the fact that there exists more than one culture, and science and/or science education can reflect an individual's culture.

In conclusion, the link between culture and science has been established, and this is based on two factors. The first factor is that there exists more than one culture in the world rather than a universal culture. The second factor is that the culture has influence on science education. The link between culture and science built by this sequence supports the core concept of this thesis, and shows that the research question is a valid one. In the following Section (Section 2.3.4), the works conducted on IS and Cultures are presented.

2.3.4 Studies of Culture, Science, and Systems

A review of literature does not identify a major debate within IS as to the nature of its underlying scientific principles or the need to consider the effect of culture within them, although this kind of argument still exists within science education (Cobern and Loving 1998). This may be due to the highly grounded and applied nature of IS research since the same universalist arguments about the acultural nature of science could still be applied within the discipline since most Western (and many non-Western) IS and CS researchers were taught a modern Western 'scientific' worldview. This is still found in most science classrooms and it is this kind of worldview around which science curricula has been developed. This Western scientific world view, founded on empiricism and rationalism, is encapsulated in the words of the American National Science Teachers Association (1998) as "*Science is a method of explaining the natural world. It assumes the universe operates according to regularities and that through systematic investigation we can understand these regularities. The methodology of science emphasizes the logical testing of alternate explanations of natural phenomena against empirical data. Because science is limited to explaining the natural world by means of natural processes, it cannot use supernatural causation in its explanations. Similarly, science is precluded from making statements about supernatural forces because these are outside its provenance. Science has increased our knowledge because of this insistence on the search for natural causes.*".

Most of the research cited on culture in Chapter 2 above draws on the understanding of the effect of culture in IS, and more generally in ICT, of Hofstede (1980). His foundational work determines a culture-value by assigning cultural dimensions to a particular group of people and is widely referenced (e.g. Dafoulas and Macaulay 2001; Vogel *et al* 2001; Straub *et al* 2002; Rathod and Miranda 1999; Cagiltay 1999).

An examination of Hofstede's analysis shows that is that it is relatively simplistic in a globalised, distributed cross-cultural, computing environment since originally he identifies only four factors (dimensions) by which one culture is differentiated from another (later he adds a fifth). These are *power distance, collectivism versus individualism, femininity versus masculinity* and *uncertainty avoidance.* Hofstede's methodology involved interviewing large numbers of employees of IBM internationally and questioning them about issues such as their opinion of their supervisor's decision making style. From this data, he produced cultural indicators (quantifiers) for many nationalities.

In the following two sub-sections (Section 2.3.4.1 and 2.3.4.2), the works of Slay and Hofstede are presented. Slay's works focus on the issues of culture and science education, and extends the work to the topics of culture, military systems, and security. Hofstede concentrates on the issues of national cultures, and technology. Their works are tangible illustrations for the relationship between culture and science. However, it is necessary to understand that their work may not cover all perspectives of the relationship between culture and science since an investigation into culture related issues can be a PhD thesis in itself. Their work is only helpful in clarifing some of the underpinning concepts of this research.

2.3.4.1 Slay's Works

Slay focused on cultural issues within conceptualisations of nature, science education and military security. Expressed in her work is the fact that culture is different from country to country, and is one of the factors which is able to affect science education and information system development (e.g. military command and control system). This is especially important for this thesis, since this argument has been adapted as the foundation to build the link between culture and science.

Qualitative research into science and culture is not traditionally under taken by scientists. Criticisms may be made to suggest that the science is acultural. However, an example can be given to show that the criticisms are not correct. On September 11th 2001, two jet planes crashed into the World Trade Centre in New York. This event shocked Western minds in particular. They had developed many advanced weapons and establish sophisticated facilities to prevent missiles attacks, and nuclear damages.

Nevertheless, they have no ability to detect and to prevent this type of attack, since this type of suicide weapon (jet plane) was never an issue in their minds since this type of sacrifice does not necessarily arise in Western culture. How could an individual immolate himself for an abstract concept based on a belief system or culture?

From the example of 911, several discoveries are found. Firstly, the concept of culture is not universal. Not every person in the world accepts Western convictions. What is acceptable in one culture may not be agreed in another culture. Secondly, although cosmetically it seems that some issues do not have any connection with culture, culture in fact entirely influences an individual's daily life. Culture is how people think, and how they behave.

Slay has spent around 10 years for the research associated with cultural issues, and her works can be mainly classified into three categories. The first category expresses that Australian and Taiwanese perspectives have different explanations for the conceptualisations of nature. In addition, the second category focuses on the issue of culture and science education. Lastly, the third category puts emphasis on the issue of culture and IS. Section 2.3.4.1.1, 2.3.4.1.2, and 2.3.4.1.3 discuss these three topics separately. These works show that science is not completely independent, and provide tangible proof to demonstrate that culture is one of important factors which can influence applications of science.

However, before any further discussions, a term '*worldview*' which is used by Slay needs to be clarified. According to Slay (2001), a statement which described the relation between culture and worldview can be found as "*The terms, Worldview, and culture are often used interchangeably. It is important to realise that, once 'culture' has been defined, then members of a particular cultural group will share a common worldview*.". This means that the meaning of worldview shares the same core concept as the essence of culture, and describes a cultural view of an individual's world. In addition, there is also a critical perspective needs to be elucidated. It is not the aim of this thesis to explain the difference between Chinese and Western cultures (worldviews). It is not the intention of this research to suggest how cultural differences will shape the development and practice of computer forensic applications. It is not the purpose of this thesis to determine that which particular part of the culture differences will result in a particular

adaptation in practice. Conversely, this research does point out cultural and worldview differences that will result in alternative design of computer forensic applications.

2.3.4.1.1 Culture and Conceptualisations of Nature

Slay's PhD thesis (Slay 2000b) introduced Western and Chinese worldviews, and further discussed issues of culture and conceptualisations of nature based on these two different worldviews. This thesis lists the two worldviews defined by Slay, and adds additional explanations of the differences between a Chinese worldview and a Taiwanese worldview.

In Slay's PhD thesis (Slay 2000b), she used the Western scientific worldview discussed above and provided by American National Science Teachers Association (American National Science Teachers Association 1998) as her fundamental argument. She also stated that a Chinese worldview is deeply based on Confucianism because it is the main educational trend since the Han Dynasty (206BC-220AD). The core concept of Confucianism (Legge 1893) focuses on the relationship between man, nature, and the heavens rather than concentrating on the value of science as defined in a Western sense. In addition, Confucius established 5 social relationships, and they are *father and son*, *ruler and subject, husband and wife*, *elder and younger brother*, and *friend and friend*. In Confucius's theory, hierarchy is respected and the relationship between a supervisor and his or her subordinate is esteemed. This theory also infers the importance of interpersonal relationship.

In Confucian theory, mathematics also played an important role in defining the skills (one of six arts) needed by an educated person of this time; this is really the only direct reference to the need for scientific ability that can be drawn from Confucius since mathematics can be seen to underpin science. However, the mathematics of the time was fairly traditional.

Confucianism is one of the original arguments explained in Slay's PhD thesis as a basis for a Chinese worldview. In addition, Slay in discussing the nature of Chinese science introduced the developments of scientific theories and concepts as well. For example, Slay (2000b) reported that "*Reference is made to the possession of a primitive calendar and the evidence of astronomical and meteorological observations and mathematical*

developments such as the decimal system and multiplication tables.", and discussed the importance of the Doctrine of the Five Elements (metal, wood, water, fire, and earth) for Chinese traditional science. Nevertheless, Slay (2001b) pinpointed that the scientific theories and concepts in China are different from Western scientific values, and stated that "*It was not until 1904 and the development of the May 4th movement (and of which Lu Xun as famous writer played a part) that Western scientific thought became important in China.*". Slay's statement matches the arguments proposed by He *et al* (1991). He *et al* (1991) stated that "*Western knowledge was introduced into China which was good at observation but poor at generalisation; and hence wise people would reason that there must still be imperfections in their observation.*", and "*Truth or falsity of a scientific theory lay not in whether or not it reflected accurately the laws of change of the objective world, but rather whether or not it more conveniently served or suited a subjective hypothesis.*". In short, the above discussions prove that differences do exist between Chinese traditional science and Western science. In this thesis, the meaning of the term 'science' is Western science rather than Chinese traditional science.

Besides a Chinese worldview and Chinese scientific concepts, Slay also introduced the imperial examination, which plays a significant role in Chinese culture. Imperial examination has lasted for 1300 years (605AD-1905AD) (Haifeng 2006) in Chinese history, and had become an important part of Chinese culture.

The following statements establish the relationship between Chinese worldview and Taiwanese worldview. Biggs (1996) stated that "*Observers remark that such conditions are rare in classrooms in East and Southeast Asia, specifically those Ho (1991) refers to as 'Confucian-heritage' cultures: China, Taiwan, Singapore, Hong Kong, Japan, and Korea.*". This statement directly confirms that Taiwanese culture is deeply affected by Confucianism. In addition, the concept of imperial examination is still used in Taiwan today for high school students to enter universities. High school students need to attend an entrance examination, which is held annually, rather than applying for universities. In short, this research not only adds to the literature indicating Confucianism is the major philosophy within Taiwanese culture, but also explains that the science mentioned in Confucianism is Chinese traditional science (not Western science). Additionally, this research also demonstrates that the concept of the imperial examination is well-accepted in Taiwanese culture.

2.3.4.1.2 Culture and Science Education

Slay has published a series of papers which are associated with the issues of culture and science education. For example, Slay and Kearney (2000) pointed out that the Chinese education system is different from the Western education system, and the Chinese has unique teaching philosophy which is different from the Western teaching philosophy as well. Penetrating statement of Chinese teaching philosophy can be found in Hong (1991). Hong described that the central concept of Chinese education is that they respect elderly and books. Moreover, Chinese also respect authority, classics and experience. From this, it is realized that Chinese use their unique teaching philosophy to teach students about academic subjects, including science.

Due to the unique teaching philosophy, a Chinese mind may think differently from a Western mind, even if they face the same question. This indicates that they are likely to have different solutions and different ideas to the same question, although they both will have the same answer to the question at the end.

It is easy to say that culture and science are two independent issues. However, if the focus is put on the process rather than the result, innovative discovery may be found. An Australian and the Taiwanese may have different understandings and interpretations of multiplication although they provide the same answer of the question. This explanation is similar to the argument made by Ogunniyi (1988). Ogunniyi discovered that there are conflicts between Western and African worldview. He further argued that although Western and African science deal with the same natural world, they construct divergent cognitive interpretations to explain the natural world.

In addition, Slay (2000a) showed that different cultures and different genders are two factors which affect the students' attitudes to computers and learning. This, on the other hand, is to say that the culture is undeniably a feature that affects science applications.. Furthermore, the similar arguments can be found in the papers proposed by Slay (1998), and Cobern (1991).

2.3.4.1.3 Culture and Information System

Slay has published several papers to discuss the role of culture within an information system. For example, Slay *et al* (2003) pointed out that "*The question of culture had*

already become an important issue for researchers and users of distributed computing systems.", and listed several interesting questions. In this paper, three of them are listed below.

- "*Does national culture affect the way an individual uses the computer and the interfaces he or she might choose? Which interface elements are more problematic?*"

- "*Is there a cultural effect on the cohesiveness of distributed teams working in a technologically mediated manner across national boundaries?*"

- "*How can we develop a guide for the military of the United States of America to incorporate cross-cultural perspectives within ICT development? Would the use of the concepts of complex socio technical systems and self-organization aid in this process?*"

In this paper, the answers of previous three questions are not the primary concern, they are rhetorical. What we can learn from these three questions causes more interests. The questions imply that culture is a worthwhile issue to be studied even in the field of Information Systems. This proves the main concept of the thesis, which describes that the culture is not an independent value and has effects on the field of science.

In addition, Slay has published certain papers (Slay 2001; Slay and Burke 2001; Slay 2002) which focus on the issues of modelling of complex distributed information systems. The military Command and Control (C2) system is one obvious example of the complex distributed information systems. The meaning and the description of C2 system can be found in Slay (2002) as "*Command and control research is focused on the use of communications and computer systems in a military context with the aim being to develop appropriate technology and methodologies to allow all kinds of warfare to be won.*".

The military C2 system is used as an example to discuss about the cultural issues within information system for a good reason. This is because that the military C2 system always involves the interaction of people and information systems. In addition, in the paper, *Culture and Sensemaking in Information Warfare* (Slay 2001), a statement which

also explained the role of military C2 system can be found as "*Although the system is organised to focus on a primary task (military communications), this cannot be separated from the environment and the social factors, including cultural ones.*".

In summary, what is proved by Slay is that culture is a critical factor within the research into distributed information systems. If a C2 system is operated by the robots, the culture is not going to become an issue. This is because the robot is controlled by computer programs, and do not have its own will. However, there must be operators to activate the C2 system. Therefore the different cultural backgrounds of the operators become a serious issue, and te possible cultural issues are hence raised. This again proves that the main concept of this thesis is correct. Since the applications of computer forensics are operated by people with different cultural backgrounds, it is very likely that the cultural factors affect the applications of computer forensics.

2.3.4.2 Hofstede's Works

Hofstede proved that the differences do exist between different cultures. His findings infer two phenomena. The first phenomenon is that culture is not universal, and the cultural differences are nationally based. Hofstede (1980) proposed a term '*national culture*' to describe that each nation has its unique culture. In addition, the second phenomenon is that an individual's behaviours are indeed affected by his or her unique culture. The following two sub-sections (Section 2.3.4.2.1 and 2.3.4.2.2) give more detailed discussion of Hofstede's works.

Section 2.3.4.2.1 not only discusses the Hofstede's concept of national culture, but also introduces the five dimensions of national culture. Hofstede interprets the cultural differences between nations based on his five dimensions. The five dimensions are: *Power Distance, Individualism versus Collectivism, Masculinity versus Femininity, Uncertainty Avoidance,* and *Long-Term Orientation versus Short-Term Orientation*. In addition, Section 2.3.4.2.2 explains the data sources of these five dimensions, and proves the trustworthiness of these five dimensions.

2.3.4.2.1 Dimensions of National Culture

Hofstede (1980) proposed a term '*national culture*'. In addition, Hofstede set five dimensions for measuring national culture, and used them to evaluate the scores for

fifty-three different countries and three multi-country regions (Hofstede 2007). Based on the explanations in Hofstede and Bond (1988), the scores are relative, and the distance between lowest-score and highest-score is about 100 points. According to Hofstede (1994), the scores of the first four dimensions for each country (or multi-country regions) were based on the findings of IBM study, and the scores for the fifth dimension relied on the findings of data collected from students within twenty-three different countries. Thorough explanations of the five national cultural dimensions can be found in (Hofstede 1994), and their definitions are listed as follow.

1. Power Distance: "*This is the extent to which the less powerful members of organizations and institutions (like the family) accept and expect that power is distributed unequally. This represents inequality (more versus less), but defined from below, not from above. It suggests that a society's level of inequality is endorsed by the followers as much as by the leaders. Power and inequality, of course, are extremely fundamental facts of any society and anybody with some international experience will be aware that 'all societies are unequal, but some are more unequal than others'.*".

   According to this definition, power and inequality are two factors which can measure the cultural differences between different nations. This is understandable since hierarchy is a well-accepted in the world. Due to the design of hierarchy, people within in a group always have different status and rights.

2. Individualism versus Collectivism: "*Individualism on the one side versus its opposite, collectivism is the degree to which individuals are integrated into groups. On the individualist side, we find societies in which the ties between individuals are loose: everyone is expected to look after him/herself and his/her immediate family. On the collectivist side, we find societies in which people from birth onwards are integrated into strong, cohesive in-groups, often extended families (with uncles, aunts and grandparents) which continue protecting them in exchange for unquestioning loyalty. The word 'collectivism' in this sense has no political meaning: it refers to the group, not to the state.*

Again, the issue addressed by this dimension is an extremely fundamental one, regarding all societies in the world.".

According to this definition, the meaning of individualism shows that an individual tends to behave independently. On the contrary, collectivism points out that an individual tends to seek identification within a particular group. This concept is used by Hofstede to measure the concept of national culture.

3. Masculinity versus Femininity: "*Masculinity versus its opposite, femininity, refers to the distribution of roles between the sexes which is another fundamental issue for any society to which a range of solutions are found. The IBM studies revealed that: (a) women's values differ less among societies than men's values; (b) men's values from one country to another contain a dimension from very assertive and competitive and maximally different from women's values on the one side, to modest and caring and similar to women's values on the other. The assertive pole has been called 'masculine' and the modest, caring pole 'feminine'. The women in feminine countries have the same modest, caring values as the men; in the masculine countries they are somewhat assertive and competitive, but not as much as the men, so that these countries show a gap between men's values and women's values.*".

   The discussion of this definition shows that the value could be different between sexes even in the same culture. The sex of an individual can determine his or her behaviours and thoughts. Thus, this is a measure of the masculinity or femineity of a particular culture.

4. Uncertainty Avoidance: "*It deals with a society's tolerance for uncertainty and ambiguity: it ultimately refers to man's search for truth. It indicates to what extent a culture programs its members to feel either uncomfortable or comfortable in unstructured situations. Unstructured situations are novel, unknown, surprising and different from usual. Uncertainty avoiding cultures try to minimize the possibility of such situations by strict laws and rules, safety and security measures, and on the philosophical and religious level by a belief in absolute truth; 'there can only be one truth and we have it'. People in uncertainty avoiding countries are also more emotional, and motivated by*

inner nervous energy. The opposite type, uncertainty accepting cultures, are more tolerant of opinions different from what they are used to; they try to have as few rules as possible, and on the philosophical and religious level they are relativist and allow many currents to flow side by side. People within these cultures are more phlegmatic and contemplative, and not expected by their environment to express emotions.".

It is reasonable for people to have different level of uncertainty avoidance. Some people are willing to take the risk for unknown issues, but others are afraid of failure of unpredicted events. Consequently, it is understandable this idea is one out of five dimensions which can measure the concept of national culture.

5. Long-Term Orientation versus Short-Term Orientation: "*It can be said to deal with virtue regardless of truth. Values associated with long term orientation are thrift and perseverance; values associated with short term orientation are respect for tradition, fulfilling social obligations, and protecting one's face. Both the positively and the negatively rated values of this dimension remind us of the teachings of Confucius (King and Bond 1985). It was originally called 'Confucian dynamism'; however, the dimension also applies to countries without a Confucian heritage.*".

   The concept of this definition is deeply affected by Confucianism, which is a well-accepted theory within Chinese culture. Thus, the concept of this dimension is suitable for this research, since Taiwanese culture is part of Chinese culture. In addition, Hofstede proved that the concept of this dimension is also appropriate for other countries. In summary, Hofstede believes this concept is able to measure the concept of national culture.

Table 2 provides the Australian score for each dimension, and also lists the Taiwanese score for the same dimensions. The source of the scores is Hofstede (Hofstede 2007). According to these scores, two standpoints are confirmed. The first standpoint points out that Australia and Taiwan do not share the same culture. The second standpoint demonstrates that Australian and Taiwanese behave differently.

Table 2: Hofstede's Scores for Australia and Taiwanese cultures

	Power Distance,	Individualism versus Collectivism	Masculinity versus Femininity	Uncertainty Avoidance	Long-Term Orientation versus Short-Term Orientation
Australian Score	36	90	61	51	31
Taiwanese Score	58	17	45	69	87

2.3.4.2.2 Data Sources of Five Dimensions of National Culture

In the previous section (Section 2.3.4.2.1), this thesis showed that Hofstede (1980) proposed the concept of national culture. However, Hofstede (1980) admitted that "*the concept of national culture or national character has suffered from vagueness.*", and also stated that it is very difficult to use correct characteristics to describe the meaning of national culture. Fortunately, the author had a great opportunity to develop a large research project for over six years, from 1967 to 1973, and to establish criteria to meaningfully represent cultural differences between nations. The research project was conducted in IBM subsidiaries in 20 different languages. There were 40 independent nations involved in this large research project. Hofstede (1986) stated that "*The total number of questionnaires available for analysis was over 116,000, from employees at all levels, managers and non-managers alike; most groups were surveyed twice over a four-year interval, so that the stability of differences found and trends over time could also be tested.*". He defined four criteria for measuring cultural differences, and they are called dimensions. These four dimensions are: *Power Distance*, *Individualism versus Collectivism, Masculinity versus Femininity*, and *Uncertainty Avoidance*.

Hofstede and Bond (1988) discussed the relationship between the four dimensions and national culture, and reported that "*the IBM employees represented extremely well-matched subsets from each country's population: same company, job, and education, but different nationality. If anything, cultural differences among countries outside the corporation should be larger than they would be inside, so the national culture*

differences found inside IBM should be a conservative estimate of those existing for the countries at large.".

In order to examine the validation of the four dimensions, Hofstede adopted the concept of triangulation to examine these four national cultural dimensions. Hofstede and Bond (1988) based this on the academic research conducted on 1979 (The Chinese Culture Connection 1987). Modified version of Rokeach Value Survey (MRVS) is used to form the questionnaire in this academic research. The respondents were 100 psychology students (50 males and 50 females) from 10 different countries. The results of this academic research were published at almost the same time as the IBM research. Surprisingly, the four dimensions discovered in the IBM research can be found in this academic research as well. Therefore, Hofstede and Bond (1988) concluded that "*The overlap between the two research projects was demonstrated on the scores of six countries that were represented in both samples. This overlap is remarkable because the two projects used completely different questionnaires on different populations in different years in only partly overlapping sets of countries. The agreement between the two projects was strong support for the universality of the four IBM dimensions.*".

In addition, a fifth dimension, *Long-Term Orientation versus Short-Term Orientation*, which can also represent the differences between national cultures was found in (Hofstede and Bond 1988). According to Hofstede (1994), the concept of the fifth dimension was derived from the discovery in (The Chinese Culture Connection 1987). The necessary information for constructing the fifth dimension was developed in a study conducted among students in twenty-three countries around the world, and using Chinese Value Survey (CVS) designed by Chinese scholars (The Chinese Culture Connection 1987). This made it possible to capture unique features of Chinese culture.

The findings of CVS also confirmed the first three dimensions, *Power Distance*, *Individualism versus Collectivism*, and *Masculinity versus Femininity*, discovered in the IBM research. Although the *Uncertainty Avoidance* dimension is missing in the findings of CVS, it discovered another dimension, which is the fifth dimension in the work of Hofstede (1994), to describe characteristics of the national culture. Hofstede and Bond (1988) stated the relationship between IBM research and CVS research as "*This again in spite of the completely different questions, different populations, different*

time periods, and different mix of countries." The relationship among them is listed in the Table 3.

Table 3: Corroborations for Hofstede's Five Cultural Dimensions

IBM Research	Power Distance,	Individualism versus Collectivism	Masculinity versus Femininity	Uncertainty Avoidance	
MRVS Research	MRVS Dimension 1	MRVS Dimension 2	MRVS Dimension 3	MRVS Dimension 4	
CVS Research	CVS Dimension 1	CVS Dimension 2	CVS Dimension 3		CVS Dimension 4 (which is called Long-Term Orientation versus Short-Term Orientation in Hofstede's work)

According to the information in the Table 3, the first three dimensions (*Power Distance, Individualism versus Collectivism,* and *Masculinity versus Femininity*) are confirmed by different questionnaires, different methods, different respondents, and different countries from three different pieces of research. In addition, the forth dimension (*Uncertainty Avoidance*) is proved via the same procedures from two different pieces of research.

The fifth dimension, *Long-Term Orientation versus Short-Term Orientation*, of Hofstede's work (Hofstede and Bond 1988) was discovered by the CVS research which was designed and conducted by Chinese scholars. Unlike the previous four dimensions, the situation of this dimension is unique. This dimension can only be found in the CVS research rather than IBM research or MRVS research.

2.3.5 Summary of Section 2.3

Section 2.3.2 provides the diverse definitions of culture, and chooses "*Man is an animal suspended in webs of significance he himself has spun. I take culture to be those webs and the analysis of it is not an experimental science in search of law but an interpretative one in search of meaning.*", which was proposed by Geertz (1973), as the cultural definition for this thesis. This is because Geertz's cultural definition is the one accepted by most anthropologists. Thus, its credibility and reliability are not a problem.

After introducing the definition of culture in Section 2.3.2, Section 2.3.3 further discusses the relationship between culture and science applications. The discoveries show that different cultures have certain impacts on science applications.

In addition, Section 2.3.4 mainly refers to the works of Slay and Hofstede, to prove that culture is not universal and culture can affect science applications, such as science education and IS. In short, Section 2.3 confirms two standpoints. The first viewpoint points out that culture is not universal. The second viewpoint corroborates the relationship between culture and science applications, asserting that culture has an impact on the application of science.

2.4 Summary of this Chapter

In this chapter, several critical issues in computer forensics are presented in the Section 2.2. These points include definition, purpose, procedure, and current issues of computer forensics. Furthermore, Section 2.2 also introduces certain significant points of digital evidence. The points discuss the definition and traits of digital evidence. In Section 2.2.5, it is shown that computer forensics belongs to the field of science – it is a forensic science.

In Section 2.3, the issues associated with culture are introduced. The issues discuss the definition of culture (Section 2.3.2), and the relationship between culture, science and systems (Section 2.3.3). Moreover, the research carried out by Slay (Section 2.3.4.1) and works conducted by Hofstede (Section 2.3.4.2) prove that the culture is not universal, and is able to affect the application of science.

The outcomes from these two sections point out that culture is a factor which is able to influence the science applications, and computer forensics belongs to the field of science. Therefore, it is reasonable to assume that computer forensics is very likely to be affected by different cultures. This shows that the validity and soundness of the research question.

In conclusion, the literature review not only shows that the relationship between culture and computer forensics, but also points out that this is a significant and interesting issue which is worthwhile to study. The value of this thesis is that there is no relevant research focusing on the issues between culture and computer forensics. This thesis can be considered the first research within this field.

In the following chapter, this thesis not only explains the differences between quantitative research and qualitative research, but also clarifies that a qualitative methodology is more suitable to address the needs of this research. In addition, this thesis introduces the alternative measurements which are used to examine the quality of a qualitative research. Lastly, the methods, Delphi survey and case study, used to examine the research question, are considered at great length for their suitability and appropriateness.

3 Methodology

3.1 Overview of this Chapter

The use of a proven and reliable research methodology is a vital component of research; it is the only means of producing reliable outcomes in the work produced. This chapter aims to discuss the research methodology used for this work, as a means of determining the most effective way of answering the research questions posed. This chapter not only introduces the differences between positivist research (quantitative research) and interpretivist research (qualitative research), but also presents the explanations of quality measurements, such as validity and reliability, that are applicable to this research.

This chapter is structured as follows. In Section 3.2, positivist research and interpretivist research are introduced respectively. This section simply explains the characteristics of positivist research and interpretivist research. Furthermore, these two sections not only connect positivist research with quantitative research, but also build the relationship between interpretivist research and qualitative research.

Section 3.3, titled *Choice of Methods*, introduces both quantitative research and qualitative research, and discusses the fundamental differences between the two. This section also makes the comparison of the two research methodologies in relation to this work, placing the argument that the concept of qualitative research is the most suitable alternative for use in this thesis. As this thesis aims to collect cultural data between Australia and Taiwan, a qualitative research methodology is preferable for this work.

Section 3.4, titled *Quality of Qualitative Research*, examines the quality issues of a qualitative research methodology. In particular, the concepts of research *validity* and *reliability* are two factors usually used in the quantitative research. However, they are not appropriate in the qualitative research. Section 3.4.4 introduces alternative concepts as a means of measuring the research quality. In addition, an important concept in a qualitative research is introduced in Section 3.4.5. The concept is called *triangulation*. The concept of triangulation is to use more than one method to verify the same qualitative research. Triangulation is used as qualitative research, unlike quantitative research, does not have numerical data to prove the correctness of its standpoint. In this manner, the concept of triangulation is a reasonable way to increase the credibility and trustworthiness of the results of the qualitative. Section 3.4.5 expands on this work, and

discusses the components of a triangulated study; in particular the use of Delphi survey instruments and case studies for this work.

Section 3.5 gives a greater detail for the Delphi survey instrument that is used in this research, discussing the overall purpose, characteristics, advantages, disadvantages, procedures, number of panellists, limitations, and quality of the survey instrument. The use of Delphi technique is able to obtain quick consensus from multiple experts. This is especially important for conducting a group survey.

Section 3.6 of this research discusses the other proposed method, the case study, and outlines the definition, design, data sources, data collection, and quality of case study to this work. This section also discusses the applicability of the case study to the triangulation of methods. The use of case study is able to obtain in-depth opinions from participants by personal interview. In this case, the researcher can capture participants' standpoints more precisely. This is the value of case study. .

3.2 Positivist and Interpretivist Research

Before an educated choice can be made to determine the most relevant choice of research methodology, a discussion on the two alternatives needs to be introduced.

Hirschheim (1985) provided a fundamental explanation of positivist research stating that the apparent difference and the unique feature of positivist research is that the studied phenomena and examined subjects are observed through empirical data by objective manners. In positivist research, the empirical data are always factual, truthful and unambiguous. This indicates that the observed phenomenon is independently of the research. This standpoint is further agreed by Remenyi *et al* (1998). According to Amaratunga and Baldry (2001), Remenyi *et al*. (1998) expressed the concept of positivist research as "*The positivist approach believes that the subject under analysis should be measured through objective methods rather than being inferred subjectively – through sensation, reflection or intuition.*". From this, it is realized that the quantitative research method is a typical approach to perform positivist research. Quantitative research is introduced in Section 3.3.3 of this work.

Amaratunga and Baldry (2001) used the term, '*realism*', to replace interpretivist, and stated that the core concept of realism research as "*The researcher should not gather*

facts or simply measure how often certain patterns occur, but rather appreciate the different constructions and meanings people place upon their own experiences and the reasons for these differences.". Moreover, based on the arguments provided by Remenyi *et al* (1998), and Easterby-Smith (1991), Amaratunga and Baldry (2001) said "*The realism approach tries to understand and explain a phenomenon, rather than search for external cause or fundamental laws.*". In addition, Clarke (2000) provided an explanation to describe the differences between positivist research and interpretivist research. Clarke (2000) state "*Conventional science is based on 'rational positivist' thought. This includes the presumptions that there is a 'real world', that data can be gathered by observing it, and that those data are factual, truthful and unambiguous. The 'post-positivist', 'interpretivist' philosophy, on the other hand, asserts that these assumptions are unwarranted, that 'facts' and 'truth' are a chimera, that 'objective' observation is impossible, and that the act of observation-and-interpretation is dependent on the perspective adopted by the observer.*".

From this, it is realized that qualitative research, introduced in the Section 3.3.4, is a typical approach to perform interpretivist research. There is no numerical and statistical data to represent the correctness of the research discoveries. In this type of research, the role of the researcher is not that of an objective observer any more. The researcher's standpoints and interpretations become the most valuable data. In summary, this thesis adopts an interpretivist approaches so as to interpret cultural differences between Australia and Taiwan rather than measuring the differences. In the Section 3.3, this thesis explains the detailed reason for the appropriateness of qualitative research.

Based on this work discussing both positivist and interpretive research, it seems that positivist research is not suitable for examining the research question of this thesis. This is because it is very difficult to precisely measure and to correctly describe the cultural or cognitive development of an individual, and therefore the collection of precise numeric data is not possible. On the contrary, interpretivist research is much more suited to describe cultural differences between Australia and Taiwan. Therefore this research will utilize interpretivist research as a research approach.

3.3 Choice of Methods

3.3.1 Overview of this Section

This section explains that quantitative research and qualitative research are two important but different methods within academia. The results of quantitative research are based on statistical analyses. In contrast, interpretations provided by the academic researcher are more important in qualitative research. This section further explains the reason why qualitative survey is suitable and used in this thesis. In addition, Section 3.3.3 lists the introduction of quantitative research, and Section 3.3.4 introduces the meaning of qualitative research.

3.3.2 Choices between Quantitative Research and Qualitative Research

According to Straub *et al* (2005), the ontology of quantitative research as "*The underlying view of nature that leads a scholar to conclude that quantitative research can produce knowledge is that the world has an objective reality that can be captured and translated into testable hypotheses, usually in the form of statistical or other numerical analyses*". Additionally, the explanation of qualitative research can be found in (Myers 1997) as "*Qualitative research methods were developed in the social sciences to enable researchers to study the cultural phenomena. Examples of qualitative methods are action research, case study research and ethnography*.". In summary, these two research methods are different since they view the same phenomenon from different angles. Quantitative research tends to explain every situation via statistical analyses. In contrast, the researcher's interpretations are more important in qualitative research.

Aside from brief descriptions of both qualitative and quantitative methods, Lincoln and Guba (1985) listed a table (see Table 4) to show the different axioms between quantitative and qualitative methods.

Table 4: Different Axioms between Quantitative and Qualitative Research

	Quantitative Research (Positivist Research)	Qualitative Research (Interpretivist Research)
The nature of reality	Reality is single, tangible, and fragmentable.	Realities are multiple, constructed, and holistic.
The relationship of knower to the known	Knower and known are independent, a dualism.	Knower and known are interactive, inseparable.
The possibility of generalization	Time- and context-free generalizations (nomothetic statements) are possible.	Only time- and context-bound working hypotheses (idiographic statements) are possible.
The possibility of causal linkages	There are real causes, temporally precedent to or simultaneous with their effects.	All entities are in a state of mutual simultaneous shaping, so that it is impossible to distinguish causes from effects.
The role of values	Inquiry is value-free.	Inquiry is value-bound.

The aim of this thesis is to find out any existing difference between Australian and Taiwanese cultures from a computer forensic perspective. Two problems are raised. The first problem is that the number of participants who work in the field in either country is limited. Whilst general instruments are effective for large numbers of individuals, the focus of this work is a field of work that requires the input of experts in niche areas. Such a limited number of individuals require a different research approach than that required for a large-scale data-collection system. Therefore, computer forensic experts are the participant focus of this research, and this can be further broken into law enforcement, government employees and academic researchers. The second problem is that the experts' opinions cannot be expressed properly and correctly by numerical data. An open-end questionnaire is a better way to perform the survey in this thesis. In this case, the researcher's interpretations become a very important part of this research. In short, above two problems implies that a qualitative method is more appropriate for this research.

3.3.3 Quantitative Research

The major focus of quantitative research is on numbers and numeric data. Numerical data is the main data type in a quantitative research. In addition, the numerical data is usually further analyzed by mathematical or statistical techniques. Glesen and Peshkin (1992) proposed a table (see Table 5) that compares the quantitative research with qualitative research.

Table 5: Comparisons of Quantitative Research and Qualitative Research

	Quantitative Research (Positivist Research)	**Qualitative Research (Interpretivist Research)**
Assumptions	• Social facts have an objective reality • Primacy of method • Variables can be identified and relationships measured • Etic (outside's point of view)	• Reality is socially constructed • Primacy of subject matter • Variables are complex, interwoven, and difficult to measure • Emic (insider's point of view)
Purpose	• Generalizability • Prediction Causal explanations	• Contextualization • Interpretation • Understanding actors' perspectives
Approach	• Begins with hypotheses and theories • Manipulation and control • Uses formal instruments • Experimentation • Deductive • Component analysis • Seeks consensus, the norm • Reduces data to numerical indices • Abstract language in write-up	• Ends with hypotheses and grounded theory • Emergence and portrayal • Researcher as instrument • Naturalistic • Inductive • Searches for patterns • Seeks pluralism, complexity • Makes minor use of numerical indices • Descriptive write-up
Researcher Role	• Detachment and impartiality • Objective portrayal	• Personal involvement and partiality • Empathic understanding

Contents of the above table indicate that the two different research methods explain the natural world from different viewpoints. The table provides a better understanding of the concepts of quantitative research, and demonstrates that the quantitative research

method is not suitable for this research because this thesis relies on the researcher's interpretations of experts' opinions.

3.3.4 Qualitative Research

There are several academic opinions and considerable work that discusses qualitative research, both at an introductory level and also in more depth.

An essential understanding of qualitative research was provided by Nelson *et al* (1992) as "*Qualitative research is an interdisciplinary, transdisciplinary, and sometimes counterdisciplinary field. It crosscuts the humanities and the social and physical sciences. Qualitative research is many things at the same time. It is multiparadigmatic in focus. Its practitioners are sensitive to the value of the multimethod approach. They are committed to the naturalistic perspective and to the interpretive understanding of human experience. At the same time, the field is inherently political and shaped by multiple ethical and political positions. Qualitative research embraces two tensions at the same time. On the one hand, it is drawn to a broad, interpretive, postexperimental, postmodern, feminist, and critical sensibility. On the other hand, it is drawn to more narrowly defined positivist, postpositivist, humanistic, and naturalistic conceptions of human experience and its analysis. Further, these tensions can be combined in the same project, bringing both postmodern and naturalistic or both critical and humanistic perspectives to bear.*".

Denzin and Lincoln (1994) also gave their definition of qualitative research as "*Qualitative research is multimethod in focus, involving an interpretive, naturalistic approach to its subject matter. This means that qualitative researchers study things in their natural settings, attempting to make sense of or interpret phenomena in terms of the meanings people bring to them. Qualitative research involves the studied use and collection of a variety of empirical materials - case study, personal experience, introspective, life story, interview, observational, historical, interactional, and visual texts - that describe routine and problematic moments and meaning in individuals' lives.*".

Creswell (1998) did a similar task by defining qualitative research as "*Qualitative research is an inquiry process of understanding based on distinct methodological*

traditions of inquiry that explore a social or human problem. The researcher builds a complex, holistic picture, analyses words, reports detailed views of informants, and conducts the study in a natural setting.".

Myers (1997), unlike previous researchers, only simply expressed the qualitative research as "*qualitative research methods are designed to help researchers understand people and the social and cultural contexts within which they live.*". In addition, according to (Chua 1986; Orlikowski and Baroudi 1991), the epistemology of qualitative research can be categorized into three groups, and they are positivist, interpretive, and critical. More discussions about the qualitative methods can be found in (Ezzy 2002; Strauss and Corbin 1998; Taylor and Bogdan 1998; Tesch 1990).

From these definitions and sources of discussion of qualitative research, this research concludes that the overall concept of qualitative research is the interpretation of observed scenarios. This is the unique characteristic of qualitative research. Rather than using numerical data, the researcher of a qualitative research project interprets the discoveries by his or her standpoints or understanding. This argument responds to the discussion in Section 3.3.2, and shows that the numerical data is not the prerequisite of qualitative research. The discussions presented and the definitions of qualitative research not only point out that there are numerous ways to develop qualitative research, such as fieldwork study, case study and action research These definitions also do not preclude the use of multiple methods to triangulate a more verifiable and reliable research result.

The following two sections introduce the concept of validity (Section 3.4.2) and the theory of reliability (Section 3.4.3) for a qualitative research. These two factors are used in quantitative research to measure the research outcome quality. The following two sections of this thesis examine the suitability of these concepts within a qualitative research.

3.3.5 Summary of Section 3.3

Section 3.3 demonstrates that the concepts of quantitative and qualitative research are different. The interpretations of quantitative results are mainly based on the statistical analysis. On the contrary, qualitative results are usually interpreted by the researcher. In

addition, Section 3.3.2 explains that qualitative method is more appropriate for this research. This is because this thesis focuses on the cultural interpretations of the computer forensic experts' opinions. Lastly, Section 3.3.3 and 3.3.4 introduce the characteristics and features of quantitative and qualitative research respectively.

3.4 Quality of Qualitative Research

3.4.1 Overview of this Section

This section discusses application of the terms *Validity* and *Reliability* in qualitative (interpretivist) research. Validity and reliability are two common concepts, which are normally used in the field of quantitative (positivist) research, to measure the quality of its discoveries. However, since qualitative (interpretivist) research and quantitative (positivist) research observe nature world from different perspectives, the question of the use of *validity* and *reliability* in qualitative (interpretivist) research becomes a potential issue that needs to be overcome to ensure quality metrics for this work.

In Section 3.4.2, the conventional concepts of validity in quantitative research are discussed. In Section 3.4.3, the conventional concepts of reliability in quantitative research are introduced. The aim of these two sections is to explore the roles of validity and reliability in quantitative research, and then to demonstrate that the concepts of validity and reliability are not appropriate for qualitative research. Therefore, the conventional terms '*validity*' and '*reliability*' are still used in these two sections.

In Section 3.4.4, the alternative terms, provided by Lincoln and Guba (1985), for validity and reliability are introduced. These alternative terms are the terms used in this thesis. In Section 3.4.5, the concept of triangulation is presented. The purpose of triangulation is to enhance the quality of a qualitative research.

3.4.2 Validity of Quantitative Research (Positivist Research)

The definition of validity must be introduced and explained before any further discussion of validity. According to Golafshani (2003), a fundamental understanding of validity was provided by Joppe (2000) as: "*Validity determines whether the research truly measures that which it was intended to measure or how truthful the research results are. In other words, does the research instrument allow you to hit 'the bull's*

eye' of your research object? Researchers generally determine validity by asking a series of questions, and will often look for the answers in the research of others.". In addition, De Vaus (2001) stated that the purpose of validity as "*To address the question: is the research design delivering the conclusions that we claim it delivers?*".

Moreover, the concept of validity is normally discussed by internal validity and external validity respectively. De Vaus (2001) stated the internal validity as "*We need to be confident that the research design can sustain the causal conclusions that we claim for it. The capacity of a research design to do this reflects its internal validity*.", and external validity as "*External validity refers to the extent to which results from a study can be generalized beyond the particular study.*".

Although using the concept of validity to test or to evaluate the quality of quantitative research is widespread, some academic researchers, however, do not agree to use the word *validity* within the field of qualitative research. According to Golafshani (2003), Winter (2000) expressed that "*The concept of validity is described by a wide range of terms in qualitative studies. This concept is not a single, fixed or universal concept, but rather a contingent construct, inescapably grounded in the processes and intentions of particular research methodologies and projects.*". This argument is true since many researchers, such as Davies and Dodd (2002), Lincoln and Guba (1985), Seale (1999), and Stenbacka (2001), developed their own concepts and used other terms, such as *Rigor* and *Trustworthiness*, to describe the concept of validity in qualitative research. In this thesis, the terms developed by Lincoln and Guba (1985) are adopted and are discussed in the Section 3.4.4 due to their reputation within the field.

Regardless of the different terms for the concept of validity within the field of qualitative research, it seems that academic researchers all agreed that the concept of validity can truly represent the quality of qualitative research. For example, Stenbacka (2001) admitted the importance of validity for qualitative research although Stenbacka (2001) once said that the concept of reliability is able to jeopardize the quality of qualitative research.

The concept of validity plays an important role in this thesis because Lincoln and Guba (1985) and Patton (2001) stated that reliability is a consequence of the validity in a qualitative study. They were actually saying the confirmation of the validity of a study

is enough to guarantee its quality. Therefore, this thesis gives thorough discussions about the quality of Delphi method and case study by checking their validities in the Section 3.5.9 and 3.6.6 respectively.

3.4.3 Reliability of Quantitative Research (Positivist Research)

The definition of reliability must be introduced and explained before any further discussion of the concept. According to De Vaus (2001), the meaning of reliability is given as: "*A reliable measure is one that gives the same 'reading' when used on repeated occasions.*". According to Golafshani (2003), a fundamental understanding of reliability was given by Kirk and Miller (1986) as "*1) the degree to which a measurement, given repeatedly, remains the same, 2) the stability of a measurement over time, and 3) the similarity of measurements within a given time period.*".

Moreover, the definition given by Joppe (2000) can also be found in Golafshani (2003) as "*The extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability and if the results of a study can be reproduced under a similar methodology, then the research instrument is considered to be reliable.*".

Although using the concept of reliability to test or to evaluate the quality of quantitative research is widespread, some academic researchers, however, do not agree to use the word *reliability* within the field of qualitative research. For example, Lincoln and Guba (1985) used the word '*dependability*' to represent the concept of reliability within the field of qualitative research. Furthermore, according to Golafshani (2003), Stenbacka (2001) provided a completely different point of view to describe the role of reliability in qualitative research as "*Since reliability issue concerns measurements then it has no relevance in qualitative research. She adds the issue of reliability is an irrelevant matter in the judgement of quality of qualitative research. Therefore, if it is used then the consequence is rather that the study is no good.*".

Above discussions points out that using reliability as an evaluation factor to measure the quality of a qualitative research may not be completely appropriate. The work conducted by Lincoln and Guba (1985) provided another standpoint to estimate the role of reliability in qualitative research. They stated that "*Since there can be no validity*

without reliability, a demonstration of the former (validity) is sufficient to establish the latter". Lincoln and Guba are not the only researchers have this type of argument. Patton (2001) also agreed that reliability is a consequence of the validity in a qualitative study.

Despite the disagreement for the interpretation of the term *Reliability* within the field of qualitative research, this thesis accepts the concepts of reliability provided by Lincoln and Guba (1985), Patton (2001), and Stenbacka (2001). One of the major reasons for this acceptance comes from the fact that this researcher is not able to guarantee that the results of this research may be entirely reproducible by other researchers in the event that similar research is later conducted. The rapid changes within the field of computer forensics have the capacity to change opinions, thoughts and technical capacities, and therefore the time period over which data collection is made is crucial. Later research may determine how the field is changing, but will never be able to completely recapture the essence of the current research. Therefore, this thesis focuses on validity issues rather than reliability issues in order to guarantee its quality, which is more in line with the nature of qualitative research.

The next section of this work discusses the alternative terms for *validity* and *reliability* are presented. The researchers, such as Lincoln and Guba (1985), created alternative terms for validity and reliability in qualitative research in order to solve the disagreements of using validity and reliability in qualitative research. This standpoint is currently well-accepted.

3.4.4 Alternative Terms for Qualitative Research (Interpretivist Research)

From the previous sections, it can be seen that the concepts of a qualitative research and quantitative research are fundamentally different. The concepts which are available in quantitative research are sometimes not acceptable in qualitative research. For example, there are debates about the usage of validity and reliability in a qualitative research (Davies and Dodd 2002; Lincoln and Guba 1985; Seale 1999; Stenbacka 2001). This means the terms (e.g. reliability and validity), which are normally used in quantitative research to examine its quality may not be applicable in qualitative research.

Unfortunately, the quality of a qualitative research still needs to be measured and to be discussed in order to ensure that the results are authentic and substantial. The statement made by Eisner (1991) agreed that the quality issues of a qualitative research is awkward, stating "*There are no operationally defined truth tests to apply to qualitative research.*". In addition, Strauss and Corbin (1990) also expressed a similar opinion as "*Usual canons of good science…require redefinition in order to fit the realities of qualitative research.*". Therefore, this thesis uses the alternative terms (Lincoln and Guba 1985), credibility, transferability, dependability, to measure the quality of a qualitative research. These alternative terms replace the typical words, such as validity and reliability, used in quantitative work. The Table 6 shows the relationship between these alternative terms and conventional terms.

Table 6: The Comparison of Conventional Terms and Alternative Terms

Conventional Terms	Alternative Terms
Internal Validity	Credibility
External Validity	Transferability
Reliability	Dependability

The following three sub-sections (Section 3.4.4.1, Section 3.4.4.2, and Section 3.4.4.3) introduce the relationship between conventional terms and alternative terms. In this thesis, a standpoint must be clarified. Although academic researchers use different terms in quantitative and qualitative research, their purposes are very simple and are always the same. They try to provide a better way to measure the quality of academic research, including quantitative research and qualitative research. The only difference is that they observe the natural world from different perspectives.

3.4.4.1 Internal Validity and Credibility

Since the concept of validity can be further classified into internal validity and external validity, this research discusses them separately. The fundamental understanding of internal validity is provided by De Vaus (2001) as "*We need to be confident that the research design can sustain the causal conclusions that we claim for it. The capacity of a research design to do this reflects its internal validity*." In addition, Marie (1997) also provided the definition of internal validity as "*Internal validity refers to the extent to*

which the findings accurately describe reality.". However, Lincoln and Guba (1985) stated that "*the determination of such isomorphism is in principle impossible*", since people know the '*precise nature of that reality*' before they test it. This infers that it is meaningless to have such a test. Thus, Marie (1997) sated that "*The conventional researcher must postulate relationships and then test them; the postulate cannot be proved, but only falsified. The naturalistic researcher, on the other hand, assumes the presence of multiple realities and attempts to represent these multiple realities adequately. Credibility becomes the test for this.*".

According to Marie (1997), Patton (1990) defined the credibility as "*Credibility depends less on sample size than on the richness of the information gathered and on the analytical abilities of the researcher.*". Patton (1990) further said that the concept of credibility can be addressed and enhanced through triangulation of data. The detailed concept of triangulation will be introduced in Section 3.4.5.

3.4.4.2 External Validity and Transferability

The fundamental understanding of external validity is provided by De Vaus (2001) as "*External validity refers to the extent to which results from a study can be generalized beyond the particular study.*". In addition, Marie (1997) provided the conventional definition of external validity as "*External validity refers to the ability to generalize findings across different settings.*". However, Lincoln and Guba (1985) expressed that it is impossible to generalize due to the existence of local conditions, although Lincoln and Guba both agreed that the generalizability is an interesting concept. Moreover, a similar statement was provided by Cronbach (1975) as "*When we give proper weight to local conditions, any generalization is a working hypothesis, not a conclusion.*".

According to Marie (1997), Lincoln and Guba (1985) stated the transferability as "*In the naturalistic paradigm, the transferability of a working hypothesis to other situations depends on the degree of similarity between the original situation and the situation to which it is transferred. The researcher cannot specify the transferability of findings; he or she can only provide sufficient information that can then be used by the reader to determine whether the findings are applicable to the new situation.*".

In conclusion, this explanation demonstrates that this thesis cannot be judged by the criterion of external validity (transferability) since this thesis places an emphasis on the cultural issues within the field of computer forensics and compares Australia and Taiwan. The uniqueness of each culture makes the results of this research exclusive as well. To apply the results, discovered in this thesis, to other cultures or countries is very likely to be inappropriate. Due to the focus of this research, it is claimed that the concept of external validity (transferability) is not suitable to this thesis.

3.4.4.3 Reliability and Dependability

According to Golafshani (2003), a fundamental understanding of reliability was given by Kirk and Miller (1986) as "*1) the degree to which a measurement, given repeatedly, remains the same, 2) the stability of a measurement over time, and 3) the similarity of measurements within a given time period.*". Kirk and Miller (1986) further stated that it is common for qualitative researchers to put more emphasis on validity issues of their works rather than focusing on reliability issues. Moreover, the definition of reliability given by Joppe (2000) can also be found in Golafshani (2003) as "*The extent to which results are consistent over time and an accurate representation of the total population under study is referred to as reliability and if the results of a study can be reproduced under a similar methodology, then the research instrument is considered to be reliable.*".

However, Lincoln and Guba (1985) do not accept conventional explanations of reliability within the field of qualitative research, and then provided their own interpretation of reliability in qualitative research. They stated that "*Since there can be no validity without reliability, a demonstration of the former (validity) is sufficient to establish the latter (reliability).*". This statement means that they actually stated since there can be no credibility without dependability, a demonstration of the former (credibility) is sufficient to establish the latter (dependability). Lincoln and Guba (1985) are not the only researchers have this type of argument. Patton (2001) also agreed that reliability is a consequence of the validity in a qualitative study.

In conclusion, Lincoln and Guba (1985) and Patton (2001) did not deny the importance the concept of reliability within the field of qualitative research. Instead, Lincoln and Guba (1985) created the alternative term, credibility, to discuss the concept of reliability

of qualitative research. Based on the opinions provided by Lincoln and Guba (1985) and Patton (2001), as long as the credibility of this thesis can be ensured, the dependability of this thesis is then guaranteed.

3.4.5 Triangulation

Stake (1995) asserted the definition of triangulation is "*The protocols that are used to ensure accuracy and alternative explanations are called triangulation.*". Mathison (1988) also pointed out the importance of triangulation, and defined its meaning as "*Triangulation has risen an important methodological issue in naturalistic and qualitative approaches to evaluation (in order to) control bias and establishing valid propositions because traditional scientific techniques are incompatible with this alternate epistemology.*". Moreover, Ragin (1989) in his book cited this concept as well. Mingers (2001) is another scholar who supports the theory of triangulation. Mingers (2001) stated that "*It suggests that research results will be richer and more reliable if different research methods, preferably from different (existing) paradigms, are routinely combined together*.".

According to Amaratunga and Baldry (2001), Denzin (1984) defined there are 4 types of triangulation, and they are: *Data Source Triangulation*, *Investigator Triangulation*, *Theory Triangulation*, and *Methodological Triangulation*. The explanations of each type of triangulation, referenced from Amaratunga and Baldry (2001), are listed below.

1. Data source triangulation: "*When the researcher looks for the data to remain the same in difference contexts.*".
2. Investigator triangulation: "*When several investigators examine the same phenomenon.*".
3. Theory triangulation: "*When investigators with different viewpoints interpret the same results.*".
4. Methodological triangulation: "*When one approach is followed by another, to increase confidence in the interpretation.*".

The need for triangulation is usually necessary in qualitative research, since a qualitative research normally does not have numerical data or statistic information to prove and to support the accuracy of its findings. Thus, more than one systematic

research method gives the qualitative researchers ability to prove and to claim the robust of the findings. This shows that the meaning of triangulation is that different research methods use different techniques to analyse the same problem from different angles. The weakness of method A is likely covered by the advantage of method B. Consequently, the findings are tested by several research methods. From this, researchers of qualitative research can claim that these findings are '*accurate*'.

Based on the previous discussions, it is understood that the concept of triangulation plays an important role in qualitative research. Some actual work which uses the concept of triangulation can be found in Shore and Cross (2005), and Amaratunga and Baldry (2001).

In short, the concept of triangulation can improve the quality (credibility) of qualitative research. This idea is already proved in the Section 3.4.4.1 due to the statement made by Patton (1990). Furthermore, Lincoln and Guba (1985) agreed that once the credibility of qualitative research is ensured, it means the dependability of qualitative research is confirmed as well. This infers that the triangulation plays a very important role in this thesis because the use of triangulation is fully responsible for the credibility of this thesis, and the credibility of this thesis is able to affect and decide the dependability of this thesis. In this research, three research methods are used to follow the concept of the triangulation and to prove the credibility of the findings of this research. This thesis uses literature review, Delphi method, and case study as research methods. The reasons are listed below.

3.4.5.1 Historical Data

Literature review with no doubt is a simple but effective way to prove the idea of this research. Although the literature does not provide the answer of this research, it shows that culture has influences on science applications. Since computer forensics is a branch of science, it can be inferred that culture must have impacts on computer forensics. Hence the literature review builds the link between culture and computer forensics, and points out that culture and computer forensics are interrelated. The related literature is shown in Chapter 2.

3.4.5.2 Delphi Method

Both the Delphi and case study methodologies are conducted through different types of survey technique for this research. The Delphi method is based on the answers of the questionnaire, and case study relies on interview information. Newsted *et al* (1998) state "*A survey is a way of going from observations to theory validation.*". Accordingly it is correct for this research to use survey methods to interpret the observations. Moreover, Newsted *et al* (1997) stated that "*In an interpretivist context surveys are appropriate as a complement to other forms of data or observations. They can serve as a way to add to one's knowledge through "triangulation" as one of several methods. Thus it is important to realize that while surveys are typically used in quantitative research, they can also help qualitative researchers as well.*". Consequently, the decision of using survey techniques in this thesis is correct and appropriate. In the following paragraphs, this thesis further explains the reasons for using Delphi method.

The Delphi survey instrument method is used as the research method for this research due to the reason described by Linstone and Turoff (2002). Linstone and Turoff (2002) stated that "*the individuals needed to contribute to the examination of a broad or complex problem have no history of adequate communication and may represent diverse backgrounds with respect to experience or expertise.*". In addition, Linstone and Turoff (1975) gave a view of the Delphi method as "*Delphi may be characterized as a method for structuring a group communication process, so that the process is effective in allowing a group of individuals, as a whole, to deal with complex problems.*". Furthermore, there are other researchers who agree that the Delphi technique is appropriate for qualitative research. For example, Benarie (1988) and Woudenberg (1991) agreed that the Delphi technique, a qualitative research methodology, is capability of solving problems with complex topics.

In this thesis, the Delphi method is used to collect opinions from computer forensic experts. Using Delphi method not only can survey 10 respondents at the same time, but also can obtain the consensus very quickly. However, the apparent shortcoming of the Delphi method is that a unique opinion from one of participants is very likely to be neglected due to consensus processes. Hence, case study is applied to cover the weakness of the Delphi method, and to satisfy the quality requirements of this thesis. The use of case study satisfies the triangulation need for a qualitative research as well. The thorough discussions of the Delphi method can be found in Section 3.5.

3.4.5.3 Case Study

Case study is a method commonly used in qualitative research (Orlikowski and Baroudi 1991; Alavi and Carlson 1992). Feagin *et al* (1991) stated that "*The quintessential characteristic of case studies is that they strive towards a holistic understanding of cultural systems of action.*". This is one of the major reasons why the case study method is adopted in this research, as this study seeks to discover the cultural differences between Australia and Taiwan. Moreover, current research is constantly altering and expanding the nature of what constitutes the meaning of a case study. Schramm (1971) expressed the meaning of case study as "*The essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what result*.". In addition, Yin (1989) defined the scope of a case study as "*A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.*".

Unlike the Delphi survey instrument research methodology, the use of case study in this research adopts interviews to obtain critical and necessary information from two computer forensic experts in each cultural area. One advantage of the use of a case study is the immediate feedback the researcher gains and is able to follow up which are more in-depth than the answers obtained by the Delphi survey. Therefore, the advantage of case study is able to complement the disadvantages inherent in the Delphi method. The unique opinions of a particular participant can be preserved and analysed. However, the case study methodology has its own weaknesses. It is not feasible to hold a similar number of interviews as to have Delphi survey respondents. Fortunately, this known weakness in the case study methodology is satisfied by also adopting the Delphi methodology to work in conjunction, as the participants of a Delphi survey are able to be surveyed at the same time. Thus, it can be considered that the two methods, Delphi survey instrument and case study, are complementary in this research. In addition, the use of these two research methods satisfies the need of triangulation within the field of qualitative research. The thorough discussions of case study can be found in Section 3.6.

3.4.6 Summary of Section 3.4

The quality issues of qualitative research are discussed in this section. Section 3.4.2 and Section 3.4.3 introduce the concepts of validity and reliability of quantitative research respectively in order to provide the basic understanding of these two terms. However, Section 3.4.4 explains that the fundamental concepts of quantitative and qualitative research are different. Thus, the alternative terms (credibility, transferability, and dependability) rather than corresponding conventional terms (internal validity, external validity, and reliability) are used in qualitative research. In addition, the concept of triangulation is presented in Section 3.4.5 Triangulation is a very important theory in qualitative research since the results of qualitative research cannot be statistically proved. Using multiple methods is able to enhance the trustworthiness of the results of qualitative research.

3.5 Delphi Survey Method

3.5.1 Overview of this Section

The Delphi survey method is a structured group interaction process which is designed to poll experts within a given area to achieve a group consensus on specific issues over several rounds. The usage of the Delphi survey instrument is widespread and it has several applications. For example it can be used to predict future incidents, and to produce a quick consensus of a group feedback. The Delphi technique (Dajani *et al* 1979; Ford 1975; Kendall 1977; Quaile and Fowles 1975; Riggs 1983; Rowe *et al* 1991; Woudenberg 1991) allows a researcher to collect opinions of a special topic from experts within a particular area and to overcome the limitations of other survey techniques (Okoli and Pawlowski 2004). The Delphi survey methodology centres on the obtaining of iterative responses from participants, using a series of questionnaire rounds. Each round of surveys is managed by a researcher, who collates the responses from after each round to determine the agreement by respondents, and to remove questions which are agreed to from the next. This process repeats until all these responses of every single question are converged. The reason behind this is that a researcher expects the accuracy is increasing over rounds, since the group pressures for conformity. Moreover, Custer *et al* (1999), and Uhl (1983) proposed an abbreviated version of Delphi method, which is called modified Delphi method. The discussions of modified Delphi method are shown in Section 3.5.6.

According to Gupta and Clarke (1996), the number of publications is more than 463 papers between 1975 and 1994 that used the Delphi survey method as the primary data collection instrument. This number does not include the studies using the Delphi method that were still ongoing during this time period, or where the final project artefacts were not published. For example, Duboff and Spaeth (2000) stated that "*many types of minds are better than fewer and that an iterative process is one of the best ways to figure out what might happen in the future.*". The above literature not only shows that the Delphi technique is a well-accepted method within academic research, but also indicates that the results, produced by a Delphi survey, are credible and valuable. This means that using Delphi technique in this research will produce credible l results.

Alternatively some researchers discuss the validity and the reliability of results of a Delphi study rather than only focused on the Delphi technique itself. Bardecki (1984) and Parente *et al* (1984) reported that the validity and the reliability of outcomes of a Delphi study valid, as the outcomes of a Delphi survey instrument are based on experts' judgements. In addition, Ali (2005) stated "*findings of Delphi research have been perceived credible and trustworthy because they were produced by experts in regards to the issue of concern.*". Therefore, the validity of a Delphi survey as a research methodology is dependent solely on the quality of the participants and the homogeny of the areas in which they have expertise.

Therefore, relating this issue back to the research methodology for this thesis, as long as this thesis is able to guarantee the qualifications of participants, the results produced by Delphi method are then considered credible and trustworthy. This issue will be discussed in the Section 3.5.9.1. The following sub-sections is to give a complete description of the Delphi method by introducing its purposes, characteristics, advantages, disadvantages, procedures, number of panellists, limitations, and validity as means of determining the value of this research methodology for this research.

3.5.2 Purpose of Delphi Method

The original purpose of the Delphi technique is to gain useful consensus from a military expert group on a sensitive problem (Dalkey and Helmer 1963). However, Linstone and Turoff (1975) determined that the Delphi survey technique would be equally appropriate for other areas, and suggested other possible situations where the Delphi

survey methodology would be suitable. The following situations were proposed by Linstone and Turoff (1975).

- *Gathering current and historical data not accurately known or available.*
- *Examining the significance of historical events.*
- *Evaluating possible budget allocations.*
- *Exploring urban and regional planning options.*
- *Planning university campus and curriculum development.*
- *Putting together the structure of a model.*
- *Delineating the pros and cons associated with potential policy options.*
- *Developing causal relationships in complex economic or social phenomena.*
- *Distinguishing and clarifying real and perceived human motivations.*
- *Exposing priorities of personal values, social goals.*

In addition, Woudenberg (1991) provided two common benefits of the using the Delphi method; forecasting future events, and estimating unknown parameters. Linstone and Turoff (1975) stated the purpose of Delphi method as "*Gathering current and historical data not accurately known or available.*", and Woudenberg (1991) expressed that the aim of Delphi method is to estimate unknown parameters.

3.5.3 Characteristics of Delphi Method

The Delphi survey instrument is unique as a research methodology in several ways, but the characteristics of its use may not be immediately apparent (Martin and Frick 1998). According to Martin and Frick (1998), Sackman (1974) proposed several unique characteristics of the Delphi survey technique, and these are listed as follows:

- *The data collection is via a structured, formal questionnaire administered to a group of individuals identified as appropriate subject matter specialists. There is no definitive questionnaire kind or format.*
- *The Delphi director or the participants may generate the questionnaire items. In some cases, it may be a cooperative effort.*
- *The participants receive specific instructions to ensure proper completion of the questionnaire.*
- *The questionnaire is administered to the participants on two or more occasions.*

- *All administrations of the questionnaire following the first one include statistical feedback from the previous round.*
- *The statistics are typically a measure of central tendency and one of variability.*
- *The Delphi director may solicit verbal feedback from some or all of the participants and publish that information on subsequent rounds.*
- *Individual responses are kept anonymous during all administrations of the questionnaire.*
- *The Delphi director generally requires written justification for extreme responses.*
- *The cycle of iteration and feedback continues until the Delphi director determines that a sufficient convergence of opinion is reached.*

In this research, the anonymity of participant feedback is considered the most important issue during the processes of the Delphi survey. Anonymity in the data collection process will encourage more reliable feedback from participants, who are therefore less worried about the impact of their statements. This is especially true of law-enforcement-based works, where anonymity will possibly encourage more candid answers. This anonymity will be maintained throughout the evidence collection and analysis phases of this work. This is especially important since the researcher does not plan to obtain quick consensus and it is not the researcher's intention to force participants to provide similar answers.

3.5.4 Advantages of Delphi Method

According to Hwang and Lin (1987) and Saaty (1994), the Delphi survey methodology has several explicit advantages over other, similar methodologies; anonymity for participants, asynchronous interaction, no physical constraints, and the use of expert opinion. Each of these advantages is listed as follows:

1. Anonymity of participants is able to help the surveyor to obtain more desirable feedback because no individual is going to be embarrassed due to questionable answers. Anonymity also prevents the 'group-think' phenomenon, where individuals will seek to agree with others rather than state their own opinion. Therefore, the surveyor can ensure the quality of the feedbacks, and then is able to further ensure the quality of the Delphi survey.

2. Asynchronous interaction allows participants to fill out the Delphi questionnaire at their own convenience, as long as the questionnaire is completed within the specified time period. This further infers that a face-to-face group meeting is not necessary, since the comments can be provided by email or other communications mechanism.

3. There is no physical restraint for participants since the questionnaires can be sent via email. For example, participants do not need to be concerned with logistical issues that would accompany a face-to-face meeting. The lack of a physical meeting space also assists in easily providing anonymity.

4. The Delphi method only collects opinions from selected experts. By limiting survey response to individuals who are qualified in an area, insight can be gathered in very specific areas. Moreover, the Delphi surveyor put emphasis on the feedbacks of the previous feedbacks in order to obtain more accurate feedback. Thus, the agreement of the Delphi survey can be developed quickly and precisely.

The Delphi instrument is unique as a survey form, as whilst general surveys may provide insight into a general opinion, they are, as a technique, less likely to provide deep insight into complex issues. The Delphi survey technique is also preferable in many ways to interviews, as it is a means of distilling the opinions and facts from a group of people rather than an individual.

3.5.5 Disadvantages of Delphi Method

However, whilst the Delphi survey methodology has several advantages, there are some issues that have been identified, that need to be addressed within the context of this research. Hwang and Lin (1987) stated that the Delphi technique has several disadvantages that are unavoidable within the process. These disadvantages are adequate time, the ability of participants, and the motivation of participants. The detailed explanations of the disadvantages are listed as follow.

1. Performing a Delphi survey needs adequate time. This is a serious issue for both participants and the Delphi surveyor. The time required to operate a Delphi is exacerbated by the number of rounds required, which cannot be known at the beginning of the survey. Also, from a participant's perspective, time is required to fill in the questionnaire, and each survey round can only progress at the pace of the slowest participant. In addition, from surveyor's standpoint, time is needed to analyse the feedback from each round. Moreover, at the end of the Delphi processes an overview discussion is created, and the discussion costs time as well.

2. Delphi participants must be able to read and interpret each survey question correctly. That is to say that it is important for them to understand the meanings of the questions, as, unlike an interview-type situation, questions cannot be easily explained or clarified after being presented, and unlike a survey, the need for levels of agreement require that all questions are answered correctly and with a similar interpretation. Also, participants must have the ability to be able to express their viewpoints clearly and effectively, as the each Delphi round is formed based on the feedback of previous rounds. The Delphi surveyor may encounter a serious problem if the responses from participants are not written in structured sentences.

3. Participants must have a high motivation to finish Delphi survey, otherwise the research is meaningless. If the Delphi participants are forced to participate, the responses may not have the depth or results that would otherwise be achieved. In this manner, the integrity of the entire survey may be jeopardised, as the survey rounds depend on all responses.

Whilst these risks and disadvantages are inherent in the Delphi survey process, being aware of them is the first stage of mitigating them. Despite these disadvantages, the Delphi survey instrument is a known and well established method of research.

3.5.6 Procedures of Delphi Method

The procedures of performing a Delphi survey instrument are introduced within this section. The following six stages discuss the complete processes of operating a Delphi

survey instrument. The six main stages of a Delphi survey instrument are discussed in the following paragraphs.

The first stage of a Delphi survey instrument is titled *Selecting Experts*, and to the aim of this stage is to select a pool of respondents from the expert community within a given area. This allows the practitioner to collect diverse opinions from selected experts, and therefore the backgrounds of these experts must be concerned. It allows a greater of variety of opinions and thoughts to choose experts for participation with different backgrounds (e.g. scholars and practitioners). With the experts having heterogeneous backgrounds, the appropriate number of experts is 5-10 (Clayton 1997).

The second stage of a Delphi survey instrument is titled *Deciding Delphi Questions*, and to the aim of this stage is to ask the respondents to choose the qualified and suitable questions from a question list. The surveyor is responsible for providing the list of questions, and these questions may be created by actual experiences, reviewing relevant literature, and observing relevant incidents. On the other hand, the respondents are responsible for choosing qualified and suitable questions from the list. The chosen questions are going to become the actual questions in the first round questionnaire. The communications between surveyor and respondents can be conducted by email or other communications mechanism. For example, assuming the questionnaire with 100 different questions is sent out to participants in the second stage. The surveyor does not seek for the answers of these 100 questions, but he or she is looking forward for good questions. This means that the participants are asked to choose high quality questions out of these 100 questions, and then the chosen questions will become the questions in the actual Delphi questionnaire which is going to be sent out at the third stage. The purpose of the second stage is to make sure the validity of the questionnaire. In this manner, the validity of the Delphi method can be ensured as well.

The third stage of a Delphi survey instrument is titled *First Round Delphi Questionnaire*, and to the aim of this stage is to manage the respondents' feedbacks from previous stage. After the respondents choose the appropriate questions, these questions are going to be listed in the Round One questionnaire. In addition, the surveyor has to make sure that these questions are expressed by structured sentences. The validity of the Round One questionnaire is not a problem since every question is chosen and agreed by experts.

The forth stage of a Delphi survey instrument is titled *Second Round Delphi Questionnaire*, and to the aim of this stage is to create the Round Two questionnaire in order to collect experts' further responses and judgements by sorting feedbacks from the previous (Round One) questionnaire. If the consensus of a particular question is reached in the Round One questionnaire, this question is not going to be listed in the Round Two questionnaire. This infers that the questions without convergence in the Round One questionnaire will be shown in the Round Two questionnaire. Further discussions are necessary for the questions without convergence. This is the core concept of Delphi technique.

The fifth stage of a Delphi survey instrument is titled *Consensus of Delphi Questions*, and to the aim of this stage is to repeat the third stage and the forth stage until all questions reach the consensus.

The sixth stage of a Delphi survey instrument is titled *Analysing the Feedbacks of Delphi Questionnaire*, and to the aim of this stage is to analyse and interpret the consensus provided by respondents. Thus, the researcher is able to produce his or her particular insight for this research. This is the contribution of Delphi technique.

Whilst the six stages given describe all components required of a Delphi survey, the researcher must put emphasis on the number of rounds required within a specific survey, as the response rate of questionnaires is likely to decrease with increasing number of rounds (Hwang and Lin 1987). In addition, Cetron (1969) stated that it is common for a researcher to alter Delphi method to meet individual requirements and to avoid the problem of respondent attrition. Therefore, additional attention should be put on stage two, since this stage outlined the only difference between the Delphi method (Linstone and Turoff 1975) and modified Delphi method (Custer *et al* 1999; Uhl 1983). In this research, the Delphi questionnaire is created by adopting the theory of modified Delphi method. Since the major concept of modified Delphi method is exactly the same as Delphi method, the term '*Delphi method*' used in this thesis actually has the same meaning as the term '*modified Delphi method*'. In this thesis, the major difference between Delphi technique and modified Delphi method is that the actual questionnaire of modified Delphi method is decided by the surveyor rather than the Delphi participants. The total procedures of a modified Delphi survey are shown in Figure 9.

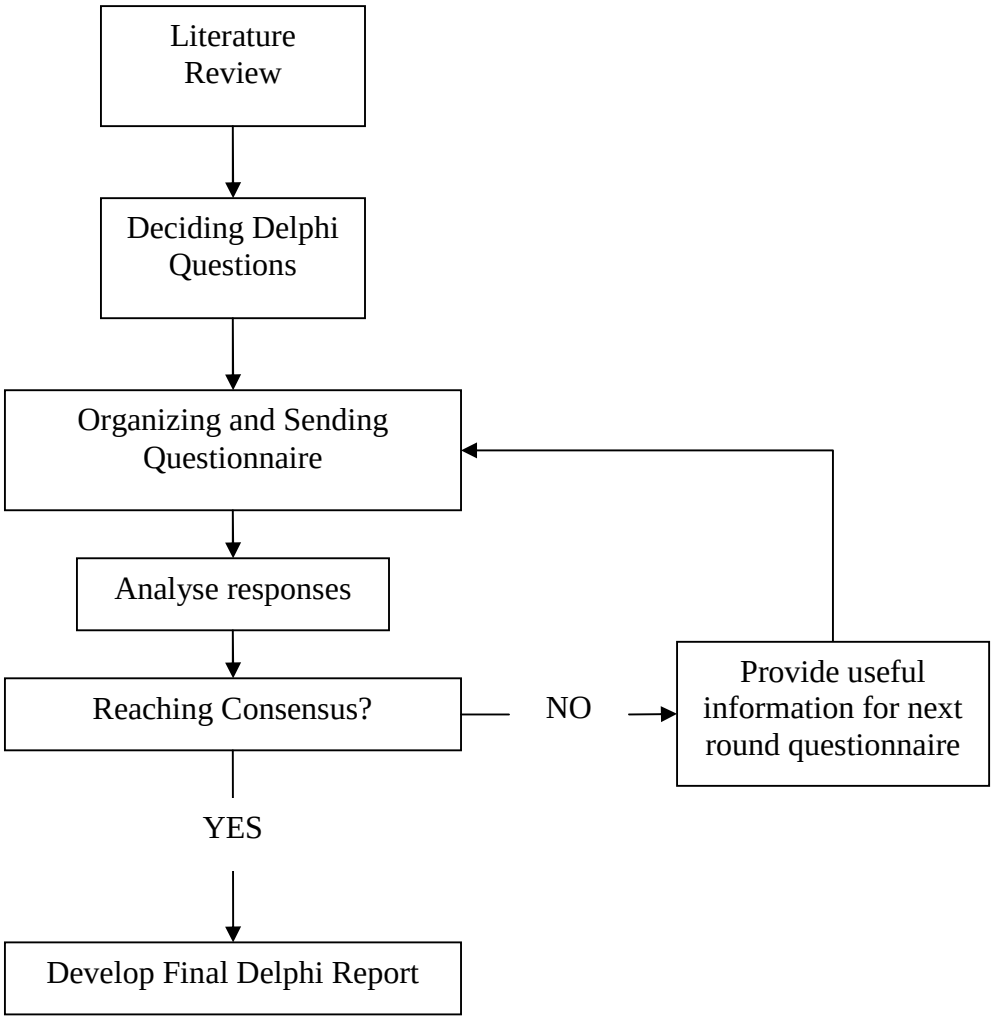


Figure 9: Modified Delphi Processes

Whilst the core aims of the modified Delphi survey method are the same as the original Delphi survey mechanism, there is a greater push for simplicity in the question creation process. The mechanism for achieving this simplicity is to omit the second stage of creating a Delphi survey, and to instead construct these Delphi questions based on actual experiences, literature review, and/or interviews of experts to form the questionnaire in third stage rather than using techniques mentioned in the second stage.

The modified Delphi survey methodology has been an accepted variation of the Delphi survey methodology, and based on the previous discussions, it has been accepted that using modified Delphi technique is not in danger of jeopardize the quality of research in which it is employed. The modified Delphi survey also has the added benefit of reducing the time required to create the initial questions, and this directly helps mitigate

one of the listed disadvantages of the methodology. As long as the surveyor can ensure the quality of the questionnaire, the quality of modified Delphi technique itself is not a problem. Section 3.5.9 discusses the quality issues with Delphi in more detail. Although the discussions are based on whole research, they are still applicable to the modified Delphi method.

Moreover, the study conducted by Reeves and Jauch (1978) showed the value of sending questionnaires more than two rounds in a Delphi process is debatable since changes made after the second round are rare. Green, Hunter and Moore (1990) also reported that sending questionnaires for two or three times in a Delphi process is enough for the experts' responses to converge. Therefore, the Delphi process in this research is going to have at most three rounds. If the responses still not reach the consensus, the underlying reason for this may need further analysis.

3.5.7 Number of Panellists of Delphi Method

There are several academic sources (Dalkey 1969; Delbecq *et al* 1986; Miller 1993; De Loe 1995; Clayton 1997; Fitch *et al* 2001) that discuss the size of a panel required to achieve a reasonable outcome within a Delphi survey. The variety of different opinions put forward by researchers indicates that there is no strict number of required participants for a Delphi survey, and that the final number is dependent on the individual survey and the outcomes sought. This research aims to survey a very narrow and specialist field of experts, it would therefore be appropriate to choose a number of experts that will give a spectrum of opinions, yet to choose a small enough number to allow fast rounds for participants. Thus, this thesis chooses a number of respondents that will be between five and ten respondents. This section further discusses this conclusion that this range of respondents is appropriate to this research.

Different academic researchers have different thoughts on the numbers of respondents required for Delphi-based research, and there is no complete or correct answer. According to Delbecq *et al* (1986), the size of a panel is changeable for a Delphi process. Delbecq *et al* (1986) further said "*With a homogeneous group of people, 10 to15 participants might be enough. Our experience indicates that few new ideas are generated within a homogeneous group once the size exceeds 30 well-chosen participants*.". Clayton (1997) asserted that if experts have similar backgrounds, to

conduct a Delphi survey needs 15 to 30 participants. On the contrary, if they have heterogeneous backgrounds, 5 to 10 participants are enough and appropriate for performing the Delphi survey. Dalkey (1969) said the consensuses of the participants' opinions keep the highest reliability and reach the minimum inaccuracy with minimum 10 people in an expert group. Fitch *et al* (2001) stated there were 9 members in the earliest RAND panels. They also said "*There is nothing magical about this number, though, and other studies have used panels ranging form 7 to 15 members.*". De Loe (1995) has stated that the number of participants should less than 50. Miller (1993) agreed that once the number of participants is more than 30, additional responses do not generate much new information.

Based on the above discussions, it is obviously that there is no universal regulation for the size of a panel when using Delphi technique. Thus, this thesis decides that the size of the panel is five to ten people with different backgrounds. This is because the number of experts in the field of computer forensic is limited since computer forensic is a fairly new research area. Furthermore, the decision is not going to affect the effectiveness of the Delphi method in this research due to the results found by Clayton (1997) and Fitch *et al* (2001).

3.5.8 Limitations of Delphi Method

Despite the several discussed unique advantages of the Delphi survey instrument as a research methodology, the technique indeed has some limitations. Some of these are discussed in Section 3.5.5. De Loe (1995) states that whilst running a Delphi survey, there are two considerations: time and effort. As an example, this research will give participants a relatively short time to complete and return each round of the questionnaire, in the range of approximately one week, and then will give the researcher another week to collect and analyse the results, and to produce the next round of the questionnaire for distribution. Therefore, with each round of the survey taking approximately one fortnight, even in ideal circumstances a survey may take 4 to 6 weeks to finish. Whilst this time period may be shortened, it can only be done so with an increase in the effort of both the researcher and participants. Considering the participants of the survey are doing this in their own time with no monetary incentive, any decrease in the time given may also decrease the quality of the answers given.

In addition to the time spent on the survey itself, the time and effort spent to manage and to analyse the feedback from each round is not a straightforward task for a researcher. After the Delphi survey rounds have completed, there is more work in the final analysis and discussion, as discovering and writing up a particular insight of the research can be regarded as the most important portion of qualitative research.

Another potential limitation of the use of Delphi as research tool has been raised in regards to converged responses of respondents. Woudenberg (1991) has stated that the produced conclusions of a Delphi survey instrument may contain inaccuracies due to participants' pressures for conformity. However, Coates (1975) argued that seeking the consensus of the responses is not the purpose of the Delphi survey. The actual aim of the Delphi survey is to give participants chances to rethink their original assumptions by forcing, cajoling, urging, or luring them, and therefore this is less on an issue than given by Woudenberg.

Ali (2005) has stated that the strengths of the Delphi technique outweigh its limitations. Ali further provided 7 suggestions to minimize problems caused by conducting a Delphi study. By adhering to these suggestions, a Delphi survey with higher quality can be produced.

1. "*Using broad questions in the first round of a Delphi survey may discourage experts with time constraints to participate in a study, which was indicated by the drop out of some participants in the first Delphi study accommodate. Less broad survey questions should be considered to stimulate expert participation in a Delphi study.*"
2. "*The time scheduled to conduct a Delphi study should be flexible to conflicting schedules of participants, and give participants sufficient time to think and rethink about issues of concern without time pressures.*"
3. "*Follow-ups are critical to have prompt responses to survey rounds. A researcher should not be discouraged by low response rates to Delphi rounds. Instead, he/she should find ways to seek more participation by sending follow-ups for each round until a required rate of response is reached.*"
4. "*Providing incentives (e.g. monetary, certificates of appreciation from a major institution, and gifts) to contributors to a Delphi study will encourage more experts to participate and respond promptly to Delphi round questionnaires.*"

5. "*Using e-mail to conduct a Delphi survey is effective, fast, and cheap, but technical communication problems in many countries, especially the developing ones, should be considered. Other methods of communication such as fax, phone calls, or regular mail can be used to conduct a Delphi survey when problems with e-mail exist.*"
6. "*Adopting majority voting as a means to analyse responses to Delphi rounds would produce reliable findings and demonstrate controversial issues, especially in large panels*."
7. "*Categorizing responses to Delphi survey (e.g. legal authority, relative autonomy, levels of control, and capacity) enabled the researcher to summarize responses to round questionnaires. That can help the analyst summarize responses to Delphi rounds when participants have diverse expertise and provide a wide range of valid responses.*"

In summary, there are a number of different research-based opinions on the use of the Delphi survey instrument, and like all research methodologies, there are limitations in its use. By understanding these, and being aware of the literature, limitations can be minimised and a strong survey developed. In the next section, this thesis is going to discuss the quality of a Delphi survey. For a high quality Delphi survey, there are two considerations: quality of participants, and quality of the Delphi questionnaire. This thesis is going to prove that the two considerations are satisfied.

3.5.9 Quality of Delphi Method

One of the major concerns with any research is to ensure that the research quality and validity is high, and within the Delphi survey instrument, this is no exception. Custer *et al* (1999) state that "*The validity of the modified Delphi process depends on the careful and systematic application of procedures for initial competency selection (e.g. reviewing the literature, developing a table of specifications, and conducting a pilot test).*". Custer *et al* (1999) used the term '*validity*' to examine the quality of modified Delphi process since Custer *et al* (1999) viewed the modified Delphi method from a Positivist perspective. However, this work is therefore not entirely applicable as this thesis is based on the concept of Interpretivist method. Thus, the term '*credibility*' is used to replace the use of '*validity*' to ensure consistency within the language used. As discussed in the Section 3.4, this research then has to adopt the concept of data source

triangulation in order to achieve the credibility. Whilst a Delphi survey instrument on its own may have disadvantages and limitations (outlined in Section 3.5.5 and 3.5.8 respectively), these can be overcome both with the production of a high quality survey and with the use of other research methodologies used to support the findings and outcomes.

In the following two sub-sections (Section 3.5.9.1 and Section 3.5.9.2), this thesis introduces the diverse backgrounds of different panellists to demonstrate that they are actually experts within the field of computer forensics. This thesis invites ten Taiwanese computer forensic experts and eight Australian computer forensic experts to participate in the Delphi survey so as to satisfy the data source triangulation.

In addition, this thesis also presents the different sources of literature from which the Delphi questionnaire is formed. These actions are able to demonstrate the concept of data source triangulation is used in this Delphi method and therefore ensure the credibility of the survey. Based on the concept provided by Lincoln and Guba (1985), this infers that the dependability of Delphi method is satisfied as well.

3.5.9.1 Quality of Delphi Panellists

When choosing participants for Delphi survey, the most concern of this thesis is the expertise and experience of selected computer forensic experts. In order to provide valuable opinions, this research cannot choose a computer forensic expert without considering his or her background and experience.

This thesis invites a number of computer forensic experts (in the region of eight to ten) to participate the Delphi survey. This number of experts was chosen for the following reasons; the number must be enough to achieve a meaningful outcome, to produce a variety of perspectives, and to satisfy the use of data triangulation within this research.

The first reason listed, that the number of participants is higher than a given minimum, comes from the fact that unless there are a certain number of participants within a Delphi, the results are meaningless. The second reason discussed is that eight to ten experts are more able to provide opinions with different perspectives. In this situation, the research can restrain any possible occurrence of bias. In addition, the third reason is

that inviting eight to ten computer forensic experts satisfies the data source triangulation (Amaratunga and Baldry 2001). These principles for the choosing of computer forensic experts are applicable for both Australian Delphi survey and Taiwanese Delphi survey.

3.5.9.1.1 Quality of Australian Delphi Panellists

Choosing panellists for the Delphi survey carefully is very significant, because as discussed in Section 3.5.7, the choice of panellists in a Delphi survey can greatly influence the outcomes of the Delphi survey. Due to the uniqueness of computer forensics, Australian panellists were invited because of their professional backgrounds. This thesis invites eight Australian panellists to participant in the Delphi survey, and to express their additional opinions. Five of them have academic backgrounds, and the other three panellists are computer forensic analysts and/or practitioners, who belong to either the law enforcement community or to a private company.

The diverse backgrounds of the survey respondents highlights two important facts; that all respondents are involved within the field of computer forensics, and that each has a different operational perspective and insight into the area. The first fact proves the quality of this Delphi survey. The essential foundation of Delphi survey is based on the expertise of panellists. They have to realize the discussed topic so as to provide valuable feedbacks. Thus, the quality of their opinions is not a debate issue. Additionally, the second fact not only gives this thesis a chance to have various feedbacks from different perspectives, but also increases the trustworthiness of the Delphi findings.

3.5.9.1.2 Quality of Taiwanese Delphi Panellists

As discussed in Section 3.5.7, the choice of panellists in a Delphi survey can greatly affect the outcome of the process, and therefore the choice of panellists is vitally important. Due to the uniqueness of computer forensics, this research chooses Taiwanese panellists only after careful consideration of their professional backgrounds. Within this work, four Taiwanese panellists have academic backgrounds, one Taiwanese panellist works as an assistant to the prosecutor, and the other five Taiwanese panellists are computer forensic analysts and practitioners.

The diverse backgrounds of the survey respondents highlights two important facts; that all respondents are involved within the field of computer forensics, and that each has a

different operational perspective and insight into the area. The first fact allows all respondents to be considered experts in computer forensics, and there can be no doubt of the quality of their opinions in the area. The second fact increases their value to the study, by providing different perspectives and insights into the work. As their feedbacks are diverse rather than partial, this increases the trustworthiness of this research.

3.5.9.2 Quality of Delphi Questionnaire

Due to the design of modified Delphi method, the questions of the Delphi questionnaire are obtained from earlier literature and/or actual experience without asking experts to sieve qualified questions (Custer *et al* 1999; Uhl 1983). The Delphi questionnaire is shown in the Appendix 1. The evident benefit of performing a modified Delphi method is that the pre-defined questions derive from current literature and/or actual experience. This means the respondents of the modified Delphi survey do not need to spend additional time to determine the qualified questions and also that the survey questions may adequately reflect current research issues. This modification to the survey methodology indeed improves the time consuming issue of the (original) Delphi method (Custer *et al* 1999; Uhl 1983). Given the research literature basis, the modified Delphi method is still able to guarantee the quality of questionnaire, since these questions are obtained from preceding literature and/or actual experience rather than created independently by the researcher. In the case of this research, all the questions are further checked and analysed by four computer forensic experts.

In this section, the researcher explains the structure of the Delphi questionnaire, and discusses the sources of literature that support the corresponding question. There are five dimensions, eleven sub-sections, and a total of forty different questions in the designed questionnaire; each dimension contains at least one sub-section. The five dimensions are: *Current Situation Dimension*, *Policy and Organization Dimension*, *Education Dimension, Law Dimension,* and *Personal Preference and Skill Dimension*. These dimensions are used as norms to describe the latest computer forensic situations and to compare the differences between Australia and Taiwan. The sequence of eleven sub-sections listed in the Delphi questionnaire is random. This is to prevent the respondents from realizing the intention of the questionnaire designer, and to guess the answers which are desired by the researcher. In addition, this shows that the respondents do not comprehend the relationship between five dimensions and eleven sub-sections.

For example, current situation dimension contains Sub-Section 1, Sub-Section 2, Sub-Section 3, and Sub-Section 8.

The five dimensions of the Delphi survey questionnaire are as follows; Current Situation, Policy and Organization, Education, Law and Personal Preference and Skill. Each of these is further partitioned into sub-sections to allow easier analysis by the researcher. These are as follows. In the **Current Situation Dimension**, there are four sub-sections. They are: *Conditions of Computer Forensics, Procedures of Computer Forensics, Characteristics of Computer Forensics*, and *Bottlenecks within Computer Forensics*. The **Policy and Organization Dimension** contains two sub-sections: *Organization of Computer Forensics*, and *Interaction in Computer Forensics*. The **Education Dimension** also has two sub-sections: *Certification of Computer Forensics*, and *Training of Computer Forensics Experts*. The **Law Dimension** contains only one sub-section; *Court Aspects of Computer Forensics*. The final dimension, **Personal Preference and Skill Dimension**, is comprised of two sub-sections: *Personal Preference of Computer Forensics Experts*, and *Skills of Computer Forensic Experts*. The following work discusses the influencing literature of Delphi questions, and explains them by dimensions rather than the sequence of questions listed in the Round One Delphi questionnaire. A full list of the questions developed or this study are found in Appendix 1.

3.5.9.2.1 Current Situation Dimension

The first dimension aims to determine the current situation within the field of computer forensics, to better understand what the issues are to develop baselines from which further conclusions may be drawn.

The first sub-section, *Conditions of Computer Forensics*, seeks to determine the current conditions for each of the cultural areas in this work. It does so based on several academic sources. Casey (2000), Allen (2005), Cooper (2005), and Dixon (2005) provided an overview of computer forensics. These references contain many current issues within computer forensics. This situation provides a motivation for this thesis to find out the following issues: government's perspective on computer forensic issues, participant's opinion on the current developments of within computer forensics, the time period of the existence of computer forensics, and the popularity of computer

forensics. Thus, Question 1, 2, 3, and 4 are developed to find out the answers respectively for the previous queries.

The second sub-section of the *Current Situation dimension*, titled *Procedures of Computer Forensics*, attempts to determine the current procedures within the field for comparative purposes. Question 5 and 6 discuss the issues of SOPs in the realm of computer forensics. Since literature (Pollitt 1995b; Civie and Civie 1998; Lin *et al* 2003a; Lin *et al* 2003b; Wang and Yang 2005; Reith *et al* 2002; Allen 2005) all admitted that the importance of SOPs in the computer forensic field, the researcher is curious about the current SOP situation in Australia and Taiwan. Furthermore, the researcher would like to find out the possible attitudinal differences toward SOPs between Australia and Taiwan. Where related papers discussed the issue of the SOPs, they all declared that necessity of a SOPs is significant.

In addition, the concept of Question 7 is derived from the literature (Civie and Civie 1998; Erbacher *et al* 2007) which discusses legal issues, procedural issues, and time-stamp issues. These three issues are admitted to be important within the field of computer forensics. Thus, Question 7 is built based on a comprehensive consideration of all three issues. This is because it is very likely for different legislation, different computer forensic procedures to have different answers for Question 7. Therefore, this gives the researcher motivation to find out the correct answer.

The third sub-section, called *Characteristics of Computer Forensics*, intends to discover the different characteristics of computer forensics between Australia and Taiwan. The concept of Question 8 is derived from Lee *et al* (2005). Lee *et al* (2005) ensured the integrity of digital evidence which is one of the most important characteristics of digital evidence. Thus, this research attempts to find out the different perspectives of the characteristics of digital evidence by Question 8. The idea of Question 9 and 10 is derived from the discussions of metadata of digital evidence (Buchholz and Spafford 2004; Kenneally 2004; Castigline *et al* 2007). As stated by Brilis *et al* (2001), metadata can be considered as "*Metadata is data about data and consists of information that characterizes data. Metadata are used to provide documentation for data products. In essence, metadata answer who, what, when, when, where, why, and how about every facet of the data that are being documented*". Metadata is a unique characteristic of digital evidence. The information, such as time stamps and log files, contained in

metadata may never be found in conventional or physical evidence form (e.g. paper-based evidence). This means the metadata is likely to assist (or to confuse) the computer forensic investigators to do their jobs. This is the reason why the researcher creates these two questions to find out the information about metadata. In addition, Lin *et al* (2003a) discussed the relationship among information policy and security management, crime investigation science, and computer science. In addition, Herath *et al* (2005) mentioned the relationship between computer forensics and information security. Their works show this relationship is an interesting issue. Therefore, Question 11 is developed to discover the relationship between computer security and computer forensics. Question 12 is the last question in this sub-section, and its idea is based on the social engineering section of Wolfe (2004). Social engineering allows computer forensic investigators to use different skills (non-technical skills) to obtain what they want to achieve. The researcher would like to discover '*Is social engineering a trendy method within the field of computer forensics?*'.

The eighth sub-section, named *Bottlenecks within Computer Forensics*, is looking for any difficulty within the field of computer forensics. It is possible for Australia and Taiwan to have different types of problems when computer forensics is performed. Since computer forensics is an oncoming and developing science, it is understood that this theme must encounter numerous obstructions. Literature (Casey 2002; Kruse and Heiser 2002; Wolfe 2004; Siegfried *et al* 2004) showed that encryption is a severe problem in the field of computer forensics. More literature (Ahmad 2002; Hosmer 2002; Kruse and Heiser 2002; Boyd and Forster 2004; Mocas 2004; Stevens 2004; Turner 2005; Schatz *et al* 2006) demonstrate that time is also a serious issue that must be faced by computer forensic investigators. Hence the researcher creates four questions (Question 27, 28, 29, and 30) to find out possible effects of the same issue which may be caused by different cultures. In addition, the idea of Question 31 is derived from the paper published by Chaski (2005). The author stated that "*In the investigation of certain crimes involving digital evidence, when a specific machine is identified as the source of documents, a legitimate question is, who was at the keyboard when the relevant documents were produced?*", and also provided examples to demonstrate that this problem has arisen in other investigations. Thus, the researcher realizes that this is a serious issue in the realm of computer forensics, and would like to uncover the effects of this problem which are caused by cultural differences.

3.5.9.2.2 Policy and Organization Dimension

The fourth sub-section, named *Organization of Computer Forensics*, attempts to determine the current issues which are related to computer forensic organizations. Allen (2005) and Dixon (2005) mentioned several computer forensic organizations and sources, such as International Association of Computer Investigative Specialists (IACIS) and International Information Systems Forensics Association (IISFA). Due to these computer forensic organizations, several relevant issues are considered to develop Question 13 and 14. In Question 13, the hierarchical issue of different organizations is discussed in order to find out the relationship between organizations. In addition, Question 14 tries to discover the different attitudes of law enforcement organizations. The idea of Question 15 is derived from the papers proposed by Tan (2001) and Mohay (2005). Moreover, the concept provided by Sommer (2004) echoes with the computer forensic readiness issues. These papers point out that forensic readiness is a concept must be addressed in order for digital evidence to be collected credibly and accurately. Mohay (2005) further described that forensic readiness as "*Forensic readiness is the extent to which computer systems or computer networks record activities and data in a manner such that the records are sufficient in their extent for subsequent forensic purposes, and such that the records are acceptable in terms of their perceived authenticity as evidence in subsequent forensic investigations*". In addition, Rowlingson (2004) stated the concept of forensic readiness as "*A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. In fact, there are many circumstances where an organisation may benefit from an ability to gather and preserve digital evidence before an incident occurs. Forensic readiness is defined as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation*". Based on the above descriptions, the importance of forensic readiness in the field of computer forensics is understood. Therefore, the researcher created Question 15 to find out if forensic readiness is a popular policy for government organizations or private companies. The researcher will further analyse this issue by cultural perspective. Additionally, Lin *et al* (2003a) discussed the relationship among information policy and security management, crime investigation science, and computer science. In addition, Herath *et al* (2005) mentioned the relationship between computer forensics and information security. Their works not only provide idea for Question 11, but also offer the foundation for Question 16. Question 16 seeks the relationship between computer security organizations and computer forensics issues organizations.

The ninth sub-section, called *Interaction in Computer Forensics*, tries to find out national and international interactions between computer forensic organizations. Allen (2005) and Dixon (2005) mentioned the computer forensic sources, such as IACIS and IISFA. Their works are not only useful for developing Question 13 and 14, but also helpful for providing ideas to create Question 32, 33, and 34. Issues of interactions between international organizations are shown in Question 32. Question 33 discusses issues of interactions between national organizations. Finally, issues of interaction between computer forensic experts are listed in Question 34.

3.5.9.2.3 Education Dimension

The fifth sub-section, titled *Certification of Computer Forensics*, aims to discover if there exist certifications for computer forensic experts and organizations. Meyers and Rogers (2004) have noted and criticised the lack of a professional certification in the field of computer forensics. They noted "*In order for the field of computer forensics to mature, there must be a national system for certifying individuals who claim to be professionals.*". Moreover, Jones (2004) also put emphasis on this issue by asking '*who are the experts?*'. Their works show that certifications of computer forensic experts are a serious and urgent issue needed to be solved. Therefore, Question 17, 18, and 19, are created in order to find out the current issues which are associated with certifications of computer forensic experts or practitioners.

The sixth sub-section, named *Training of Computer Forensics Experts*, focuses on the issues of training methods for computer forensic experts. Gottschalk *et al* (2005) identified that there is a paramount need for computer forensics programs to be existed in higher education. Therefore, the researcher realizes that the education and training issues are the first problem that must be solved. Question 20 is then created to reveal the attitude of the government organization/department/agency. By this question, the researcher expects to find out the different attitudes between Australian government and Taiwanese government. In addition, Yasinsac *et al* (2003) discussed the educational problems in the computer forensic field. The authors stated that proper education programs are beneficial for rapid growth of computer forensics. Hence, Question 21 and 22 are created to find out the answers of existing education programs or training methods. Based on the findings, the researcher can further discuss the different developments between Australia and Taiwan. Lastly, the concept of Question 23 is

based on the description proposed by Liu (2006). Liu (2006) mentioned that a computer forensic baccalaureate program was developed with 124 credits in fall 2005. Thus, the researcher is curious about '*how long it takes to properly train a computer forensic investigator?*'. It is possible for Australian and Taiwanese to have different opinions about this issue.

3.5.9.2.4 Law Dimension

The tenth sub-section, named *Court Aspects of Computer Forensics*, wants to realize that '*how members of the court consider computer forensic issues?*', and legal issues. Literature has focused on discussing computer forensics issues from legal perspectives in the field of computer forensics. Majority of the researchers in this field agree that to present digital evidence in a court of law is the ultimate goal of computer forensics. For example, Civie and Civie (1998) and Erbacher *et al* (2007) discussed the legal issues of computer forensics. Thus, three questions (Question 35, 36, and 38) are developed to distinguish the possible cultural differences of computer forensics between Australia and Taiwan from legal perspectives. Moreover, In Australian common law, discovery (Christopher and Hidgekiss 2006; Davies 2006) is the pre-trial phase in a lawsuit. Discovery allows one party to request documents and other evidence from the other party. However, there is no such concept in Taiwanese civil law. Therefore, this thesis developed Question 37 to discover any legal differences within the field of computer forensics between Australia and Taiwan.

3.5.9.2.5 Personal Preference and Skill Dimension

The seventh sub-section, named *Skills of Computer Forensic Experts*, attempts to find out the experts' attitudes toward the skills of computer forensics. Hash function is a particular and important method used in the field of computer forensics in order to reach the integrity of bit stream copies. As described in the Section 2.2.2.5.3, integrity is one of the most significant properties in the discipline of computer forensics. However, drawbacks are discovered in some hash functions, such as MD 5 and SHA-1 (Thompson 2005; Wang *et al* 2005; Wang and Yu 2005). Based on this reason, the researcher is curious about the experts' opinions on impacts on computer forensics caused by collisions of hash functions. This is the reason for researcher to design Question 24, 25, and 26.

The eleventh sub-section, titled *Personal Preference of Computer Forensics Experts*, wants to discover the possible attitude differences between Australian and Taiwanese computer forensic experts. Literature not only debated the issues of digital encrypted data (Casey 2002; Wolfe 2004; Siegfried *et al* 2004), such as the impacts of encrypted digital data on the field of computer forensics, but also discussed the significance of data cleaning tools in the computer forensic field (Jones and Meyler 2004). Hence, the researcher develops two questions (Question 39 and 40) to find out the attitudes of computer forensic experts toward data cleaning and data encryption tools. By realizing the attitudes, the researcher can find out the differences between Australian culture and Taiwanese culture.

From this series of questions, it is hoped that a well-rounded and balanced modified Delphi survey may be produced; one that is applicable to both cultural groups. The outcomes of this survey will go a long way to the understanding of the cultural differences and similarities between the ways Australia and Taiwan computer forensic approach.

3.5.10 Summary of Section 3.5

Section 3.5 has shown that the use of the Delphi survey instrument as a research methodology is well known and established in academic literature. Both the advantages and disadvantages of the research methodology are well known, along with its place within a larger research methodology, such as the use of triangulation. The concept of the modified Delphi method has also been introduced, and the differences as a research mechanism with the standard Delphi method and the acceptance within the research community discussed.

This section has also discussed a number of points specific to this research; the use of the modified Delphi survey, information on the number and types of respondents, and the sections of the survey questionnaire itself. The outcomes of this section have also highlighted the need to use the Delphi survey instrument within a larger framework, such as that provided by the Triangulation method.

The next section of this work, Section 3.6, discusses the case study as a research instrument, relating its use back to both Triangulation, and also as a means of expanding research beyond surveys as an information collection tool.

3.6 Case Study

3.6.1 Overview of this Section

It is necessary to completely understand the concept of the case study before it is used as a research method. The explanation of the case study is widely discussed in academic literature, and a good example of this is when Zonabend (1992) stated that a case study can be accomplished by performing particular approaches (e.g. observation, and analysis) of the case under study. In addition, the purpose and the unique characteristic of the case study are stated by Yin (1989). The purpose of the case study is "*The case study contributes uniquely to our knowledge of individual, organizational, social, and political phenomena*.", and the characteristic of the case study is "*The case study's unique strength is its ability to deal with a full variety of evidence – documents, artifacts, interviews, and observations. Moreover, in some situations, such as participant observation, informal manipulation can occur.*". Additionally, as indicated by Tellis (1997a), Tellis also agreed that "*Case studies are designed to bring out the details from the viewpoint of the participants using multiple sources of data*.".

However, case study as a research collection mechanism has encountered criticisms for several reasons. As stated by Yin (1989), there are several reasons for this; a lack of rigor in the process, inability to provide scientific generalization and also, performing the case study spends time and the results are usually substantial. In short, using case study as a research method has unique ability, but it also encounters unavoidable disadvantages in its use.

The use of case study is of interest to this research, as it is one possible research methodology that complements survey-based instruments by providing a greater depth and understanding than is possible from survey outcomes, such as Delphi survey. This section outlines the use of case study as a research methodology, discussing the definition, design, data sources, data collection, and quality and how it relates to this research.

3.6.2 Definition of Case Study

There are several accepted academic definitions of case study. For example, Schramm (1971) expressed that "*The essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what result.*". According to Tellis (1997b), Zonabend (1992) also expressed a different idea about case study, stating that "*The meaning of case study can be explained as case study is done by giving special attention to completeness in observation, reconstruction, and analysis of the cases under study.*" The difference between these two definitions is that the first is much narrower in scope, whereas the later definition seeks to create much larger image of the environment in which the case is positioned.

Moreover, Yin (1984), who is famous within the field of case study research, gave a more technical definition of a case study. He stated the definition of case study as "*A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context; when the boundaries between phenomenon and context are not clearly evident; and in which multiple sources of evidence are used.*". This definition is as broad as Zonabend's (1992), but is more academic in nature and more within the context of this research. Also, given the reputation of Yin, this case study definition is one of the more popular and accepted definitions within the research field. Therefore, this thesis adopts Yin's definition of case study.

3.6.3 Design of Case Study

Yin (1994) identified that five components of designing a case study are particularly significant. He further gave comprehensive explanations of previous five components. The five components for a successful case study are listed as follows: 1. A study's questions, 2. Its propositions, if any, 3. Its unit(s) of analysis, 4. The logic linking the data to the propositions; and 5. The criteria for interpreting the findings.

The first component titled, study questions, contains five different types of questions, which start by '*who*', '*what*', '*where*', '*how*', and '*why*'. In addition, the purpose of second component, titled study proposition, is to pinpoint the issues which should be explored in the study.

According to the description suggested by Yin (1989), "*Unit of analysis is related to the fundamental problem of defining what the 'case' is*". Additionally, Yin also expressed that the meaning of '*unit of analysis*' is associated with the way the principal research questions have been defined. Unit of analysis is normally a system of action rather than individuals, groups, communities, and organizations.

Yin (1989) did not provide clear explanations for the last two components. Instead, Yin (1989) only stated that "*The logic linking the data to the propositions, and the criteria for interpreting the findings have been the least well developed in case studies. These components represent the data analysis steps, and a research design should lay the foundations for this analysis.*", and used the work conducted by Campbell (1975) as example to demonstrate his standpoint.

The five components proposed by Yin are fundamental instructions for new case study researchers to build their case study individually. Every case study may have different purposes and achievements, but shares the same basic concept. Thus, these instructions are able to help researchers to successfully and easily design a case study.

3.6.4 Data Sources of Case Study

Yin (1989) and Stake (1995) both agreed that at least six separate sources can be used in a case study. They also stated that the multiple data sources is an important way to establish the reliability of the research. In this thesis, six data sources identified by Yin (1994) are: *documentation, archival records, interviews, direct observation, participant observation, and physical artifacts*.

Tellis (1997b) managed previous six data sources, and gave them comprehensive descriptions. Tellis (1997b) stated that the understanding of documents as "*Documents could be letters, memoranda, agendas, administrative documents, newspaper articles, or any document that is applicable to the investigation.*". From the viewpoint of source triangulation (Feagin *et al* 1991), the intention of documents is to corroborate the evidence from other sources.

Tellis (1997b) described the content of archival documents as "*Archival documents can be service records, organizational records, lists of names, survey data, and other such records.*"

Tellis (1997b) described the fundamental understandings of interview as "*Interviews are one of the most important sources of case study information. There are several forms of interviews that are possible: open-ended, focused, and structured. In an open-ended interview, key respondents are asked to comment about certain events. They may propose solutions or provide insight into events. They may also corroborate evidence obtained from other sources. The focused interview is used in a situation where the respondent is interviewed for a short period of time, usually answering set questions. This technique is often used to confirm data collected from another source. The structured interview is similar to a survey, and is used to gather data in cases such as neighborhood studies. The questions are detailed and developed in advance, much as they are in a survey.*".

Tellis (1997b) described the essence of direct observation as "*Direct observation occurs when a field visit is conducted during the case study. It could be as simple as casual data collection activities, or formal protocols to measure and record behaviors.*".

The purpose of participant observation is to allow the researcher become an active participant within the events being studied. This is an unusual opportunities for collecting data. However, since the researcher becomes a participant of the studied event, the collected data may sometimes questionable.

Tellis (1997b) described the meaning of physical artifacts as "*Physical artifacts can be tools, instruments, or some other physical evidence that may be collected during the study as part of a field visit.*". The ultimate aim of physical artifacts is to expand the perspective of the researcher.

In summary, six different data sources have their unique characteristics, but have distinctive weaknesses. Therefore, this is to encourage the case study researcher that he or she should try to use as many sources as possible to increase the trustworthiness of the case study. According to Tellis (1997c), Table 7, which is provided by Yin (1994), shows the advantages and disadvantages of six unique sources.

Table 7: Advantages and Disadvantages of Different Data Sources

Source of Evidence	Advantage	Disadvantage
Documentation	• Stable: repeated review • Unobtrusive: exist prior to case study • Exact: names etc. • Broad Coverage: extended time span	• Retrievability: difficult • Biased selectivity • Reporting bias: reflects author bias • Access: may be blocked
Archival Record	• Same as above • Precise and quantitative	• Same as above • Privacy might inhibit access
Interview	• Targeted: focuses on case study topic • Insightful: provides perceived causal inferences	• Bias due to poor questions • Response bias • Incomplete recollection • Reflexivity: interviewee expresses what interviewer wants to hear
Direct Observation	• Reality: covers events in real time • Contextual: covers event context	• Time consuming • Selectivity: might miss facts • Reflexivity: observer's presence might cause change • Cost: observers need time
Participant Observation	• Same as above • Insightful into interpersonal behaviour	• Same as above • Bias due to investigator's actions
Physical Artifact	• Insightful into cultural features • Insightful into technical operations	• Selectivity • Availability

As can be seen from Table 7, there are a number of advantages and disadvantages to each form of artefact used, and it is only through the use of multiple methods, or when used in conjunction with other research methodologies that may help mitigate the disadvantages that are inherent within the examination of each artefact.

3.6.5 Data Collection of Case Study

As discussed, the data collection methods used as part of the case study methodology is an important component of the method. The data collection principles introduced by Yin (1989) (discussed in Section 3.6.4) affirm this. Additionally, this work states that if a researcher uses these principles properly, the construct validity and dependability (reliability) of a case study can be increased. The quality of a case study will be further discussed in Section 3.6.6. However, the work of Yin (1989) serves as a foundation for this, citing three data collection principles for use in a case study methodology. These data collection principles are; *the use of multiple sources of evidence*, *use of a case study data base*, and *the maintaining a chain of evidence*.

The purpose of using multiple sources of evidence within a case study is to comply with the standard of data source triangulation. The thorough discussion of triangulation can be found in Section 3.4.5. As this section discusses, the findings, discoveries, and conclusions in a case study are more accurate if several different data sources are used. Furthermore, using multiple data sources can addresses the problems of construct validity, credibility (internal validity), and dependability (reliability), since multiple data sources use different evidence to describe and to prove the same phenomenon.

The meaning of and reasoning behind the need for a case study data base can be found in Yin (1989) as "*Every case study project should strive to develop a formal, retrievable data base, so that in principle, other investigators can review the evidence directly and not be limited to the written reports. In this manner, the data base will increase markedly the reliability of the entire case study.*". In addition, Yin (1989) gave the meaning of a Chain of Evidence within the research as "*An explicit link between the questions asked, the data collected, and the conclusions drawn*".

In this thesis, the concept of multiple sources of evidence and the idea of chain of evidence are used in order to provide a higher quality of this case study. As mentioned above, these two techniques are the important and essential for ensuring the construct validity, credibility (internal validity), and dependability (reliability) of a case study. Once the three measurements are ensured, this thesis can therefore be held in a high esteem.

3.6.6 Quality of Case Study

The researcher is ultimately responsible for proving and ensuring the quality of this research, the case study is no exception to this. As with other forms of research, validity and reliability are the two bases for testing the trustworthiness of a case study research. Yin (1989; 1994) defined three forms of validity that are applicable to cast study research. These forms of validity are construct validity, internal validity, and external validity. Yin (1994) used conventional terms to describe the quality of case study because their research viewed the case study from a positivist ideological perspective. On the contrary, this work approaches the case study research component from an interpretivist perspective. Therefore, as discussed in Section 3.4.4, the conventional terms used by Yin (1994) are not entirely suitable for this research, although many of the concepts raised are of use within this work. The alternative words introduced in Section 3.4.4 (credibility, transferability, and dependability) are used to clearly express the quality of the case study.

Of the terms introduced by Yin (1994), construct validity is of particular note, as the work of Lincoln and Guba (1985) does not provide an alternative concept to replace this idea. Therefore, the term *Construct Validity* is still applicable to this thesis. This indicates that this thesis should explore the concept of construct validity with additional care. Yin (1989) expressed construct validity as "*Establishing correct operational measures for the concepts being studied*.". However, Yin (1989) and Tellis (1997b) both agreed the concept of construct validity is problematic in case study research. Yin (1989) stated "*People who have been critical of case studies often point to the fact that a case study investigator fails to develop a sufficiently operational set of measures and that 'subjective' judgments are used to collect the data.*". In addition, Yin also proposed solutions for this situation, and the solutions to overcome this dilemma are: *using multiple sources of evidence*, *establishing a chain of evidence*, and *having a draft case study report reviewed by key informants*. In short, if multiple sources of evidence are used in this case study, the concept of construct validity is satisfied.

In order to ensure the credibility of this case study, this research must adopt the concept of data source triangulation as discussed in Section 3.4.5 of this work. In the following two sub-sections (Section 3.6.6.1 and Section 3.6.6.2), this research introduces the diverse backgrounds of interview respondents to demonstrate that they are experts of an appropriate calibre within the field of computer forensics. The approach of this research

is to invite two computer forensic practitioners to participate in the case study interviews so as to satisfy the data source triangulation. The sources of this questionnaire help to reaffirm the concepts of data triangulation, which also affirms construct validity and credibility of the case study. Based on the concept provided by Lincoln and Guba (1985), this infers that the dependability of case study is satisfied as well.

3.6.6.1 Quality of Case Study Participants

When choosing participants for the case study in this research, one issue that must be addressed within this thesis is the expertise and experience of selected experts. In order to provide valuable opinions, this research cannot choose a computer forensic expert without considering his or her background and experience, as experts of the highest professional calibre will be in a position to provide the greatest valuable insight.

This thesis invites two computer forensic experts to participate in the case study interview, and introduces them anonymously. This number was chosen for two reasons; two experts are able to provide various opinions and therefore minimise personal bias from any single individual, and also inviting two experts satisfies the data source triangulation required for this thesis (Amaratunga and Baldry 2001). The above principles of choosing computer forensic experts are applied for both Australian case study and Taiwanese case study.

3.6.6.1.1 Quality of Australian Case Study Participants

The case study for this research chooses Australian computer forensic experts with practical backgrounds and experiences as case study participants for the following two reasons. The case study participants must thoroughly understand the current situation within the field of computer forensics. Thus, the computer forensic practitioners are more eligible and/or suitable to do this job than academic computer forensic experts. Moreover, case study, unlike Delphi survey, seeks in-depth answers of computer forensic situations. It is easy for computer forensic practitioners to provide such answers by describing their daily works and actual experiences. This makes the computer forensic practitioners the best choice for this case study.

3.6.6.1.2 Quality of Taiwanese Case Study Participants

The case study for this research chooses Taiwanese computer forensic experts with practical backgrounds and experiences as case study participants for the following two reasons. The first reason is that this case study seeks the understandings of the current computer forensic situations. The computer forensic practitioners are more eligible and/or suitable to do this job than academic computer forensic experts, since this is what they do everyday. The second reason is that this case study looks for the in-depth answers of computer forensic situations. This again makes the computer forensic practitioners the best choice for this case study.

3.6.6.2 Quality of Case Study Questionnaire

This thesis uses two steps to ensure the quality of case study questionnaire. The first step is to create questions based on earlier literature. In addition, the second step is asking four computer forensic experts to check the quality of the questionnaire. These experts include two Australian experts and two Taiwanese experts. Similar in nature to the design of the modified Delphi questionnaire, the case study interviews are comprised of five dimensions; *Current Situation Dimension, Policy and Organization Dimension, Education Dimension, Law Dimension, and Personal Preference and Skill Dimension,*. In this section, the researcher discusses the intended outcomes of each of these dimensions and discusses the influencing literature for this work for each question. These dimensions are used as baselines to discover the latest computer forensic situations and to compare the differences of computer forensics between Australia and Taiwan. There are 13 different questions in the case study questionnaire, and the full questionnaire is shown in the Appendix 12.

3.6.6.2.1 Current Situation Dimension

The SOPs is a well-known issue within the field of computer forensics, and its importance is not debateable. Literature (Pollitt 1995b; Civie and Civie 1998; Lin *et al* 2003a; Lin *et al* 2003b; Wang and Yang 2005; Reith *et al* 2002; Allen 2005) proved this standpoint. Thus, the researcher uses Question 1 to discover the current situation of computer forensic SOPs within the participant's organization.

The idea of Question 2 is derived from Association of Chief Police Officers (2003). The researcher is interesting in the impacts of two different situations mentioned in this question since there is usually no clear regulation for a traditional investigator. The purpose of this question is to find out the possible differences between Australia and Taiwan.

Gottschalk *et al* (2005) identified that there is a paramount need for computer forensics programs to be existed in higher education. This causes researcher's interests about the number of manpower within the field of computer forensics. Question 3 is then created based on this situation.

Jones (2004) discussed the issue about the accreditation and certification of a computer forensic expert. Thus, Question 4 was created to find out the sources of qualified computer forensic practitioners.

3.6.6.2.2 Policy and Organization Dimension

Literature shows that computer forensics is a multi-disciplines subject rather than pure science. For example, Civie and Civie (1998) and Erbacher *et al* (2007) discussed the legal issues of computer forensics. This makes the researcher think about that the attitudes of computer forensic experts may be affected by the completeness or incompleteness of a law which is associated with computer forensics. Thus, Question 5 was created.

Allen (2005) and Dixon (2005) mentioned several computer forensic organizations and sources, such as IACIS and IISFA. Therefore, Question 6 was created to find out the existing organizations in Australia and Taiwan. The answers can be used to evaluate and to compare the development of computer forensics in Australia and Taiwan.

3.6.6.2.3 Education Dimension

Meyers and Rogers (2004) and Jones (2004) both put emphasis on the professional certification in the field of computer forensics. Their works points out that the proper certifications of a computer forensic expert are very important. Thus, Question 7 and Question 8 were developed to discuss the latest situations.

Gottschalk *et al* (2005) identified that there is a paramount need for computer forensics programs to be existed in higher education. Moreover, Yasinsac *et al* (2003) also discussed the educational problems in the computer forensic field, and they further stated that proper education programs are beneficial for rapid growth of computer forensics. Therefore, the researcher realizes that the educational issues are the first problem that must be solved. Thus, Question 9 was created to find out the current situations in Australia and Taiwan.

3.6.6.2.4 Law Dimension

Literature has focused on discussing computer forensics issues from the legal perspective. The majority of the researchers in this field agree that to present digital evidence in a court of law is the ultimate goal of computer forensics. For example, Civie and Civie (1998) and Erbacher *et al* (2007) discussed the legal issues of computer forensics. Thus, two questions (Question 10 and 11) are created to find out the necessity for computer forensic experts to understand legal issues or for members of the court to understand computer forensic issues.

3.6.6.2.5 Personal Preference and Skill Dimension

Literature not only debated the issues of digital encrypted data (Casey 2002; Wolfe 2004; Siegfried *et al* 2004), such as the impacts of encrypted digital data on the field of computer forensics, but also discussed the significance of data cleaning tools in the computer forensic field (Jones and Meyler 2004). Hence, the researcher developed Question 12 in order to find out the attitudes of computer forensic experts toward data encryption and data cleaning tools. By realizing the attitudes, the researcher can find out the differences between Australian culture and Taiwanese culture.

Yasinsac *et al* (2003) discussed educational problems in the computer forensic field. The authors stated that proper education programs are beneficial for rapid growth of computer forensics. Based on opinions proposed by Yasinsac *et al* (2003), Question 13 was developed to discover how technical skills of computer forensic experts be upgraded?

3.6.7 Summary of Section 3.6

Section 3.6 shows that the case study as a research methodology. The features of a case study research include definition (Section 3.6.2), design (Section 3.6.3), data sources (Section 3.6.4), data collection (Section 3.6.5), and quality (Section 3.6.6). Essential knowledge for understanding the meaning of case study is listed in this section. The quality of cast study participants and questionnaire is discussed in this section as well. This is because the trustworthiness of case study interviews is deeply based on the quality of case study participants and questionnaire. In order to provide high quality research results, this thesis discusses the backgrounds of case study participants and the quality of the case study questionnaire with additional cares.

3.7 Summary of this Chapter

The purpose of Chapter 3 was to discuss the research methodology used for this work. This chapter not only introduced the differences between quantitative research and qualitative research (Section 3.2), but also pointed out that a qualitative method is more appropriate for this research (Section 3.3).

In Section 3.4, the measurements for qualitative research are listed. Since qualitative research is different from quantitative research, conventional concepts (e.g. validity and reliability), which are suitable for quantitative research, are no longer accepted in qualitative research. Thus, the alternative terms (e.g. credibility, transferability, and dependability) proposed by Lincoln and Guba (1985) are used to examine the quality of this thesis. In addition, the concept of triangulation is introduced in Section 3.4.5. The triangulation of this thesis is achieved by combining historical data, Delphi method, and case study. Using three different research methods is able to confirm the trustworthiness of the findings of this thesis.

In Section 3.5, the details of Delphi survey method are introduced. These details include purpose (Section 3.5.2), characteristics (Section 3.5.3), advantages (Section 3.5.4), disadvantages (Section 3.5.5), procedures (Section 3.5.6), number of panelists (Section 3.5.7), limitations (Section 3.5.8), and quality (Section 3.5.9) of Delphi survey method. In addition, Section 3.5.9 is further classified into two sub-sections (Section 3.5.9.1 and 3.5.9.2) to discuss the quality of Delphi panelists and quality of Delphi questionnaire.

By understanding the quality requirements of the Delphi survey, the results of Delphi survey are able to be ensured.

In Section 3.6, the details of case study are introduced. These details include definition (Section 3.6.2), design (Section 3.6.3), data sources (Section 3.6.4), data collection (Section 3.6.5), and quality (Section 3.6.6) of case study. In order to discuss the quality issues thoroughly, Section 3.6.6.1 and 3.6.6.2 are further created. In Section 3.6.6.1, the quality of case study participants is discussed. In addition, Section 3.6.6.2 focuses on the quality of case study questionnaire. By ensuring the quality of case study participants and questionnaire, the outcomes of the case study are trustworthy.

In summary, Chapter 3 explains the essential differences between quantitative research (positivist research) and qualitative research (interpretivist research), and also introduces the alternative terms (e.g. credibility, transferability, and dependability) for examining the quality of qualitative research. In addition, the features of two research methods (Delphi survey and case study) are introduced and explained. By understanding these features, it is realized that Delphi survey and case study are suitable for this thesis.

In the following chapter, this thesis introduces the Australian Delphi survey and case study. Moreover, the cultural interpretations for the findings of Australian Delphi survey and case study will be explained as well.

4 Research Findings in Australia

4.1 Overview of this Chapter

This chapter introduces the results of the Australian Delphi survey, and the findings of two Australian case studies. In addition, cultural interpretations for these findings are provided and discussed in this chapter. The results of the Australian Delphi survey and two Australian case studies are listed in Section 4.2.2, 4.3.1.1, and 4.3.2.1 correspondingly. The Delphi outcomes are shown by dimensions which have been developed in this thesis so as to provide a better and clearer understanding of the latest situation within computer forensics in Australia. The results of an Australian case study developed to extend the survey work are listed and discussed by dimensions too.

Interpretations of the Delphi results are provided in Section 4.2.3, and these have been made to elucidate the Delphi results from a cultural perspective. Similar cultural interpretations of two Australian case studies' outcomes can be found in Section 4.3.1.2 and.4.3.2.2. Lastly, Section 4.4 combines the cultural interpretations of the Delphi outcomes with the cultural interpretations of the case study results, and provides overall conclusions for the modern situation within computer forensics in Australia. These conclusions will be further used to compare with the Taiwanese conclusions in Chapter 6 so as to produce a cross-national discussion.

4.2 Delphi Survey

In order to have valid and applicable outcomes, a Delphi survey needs be conducted with a reasonably large group of respondents (Delbecq *et al* 1986; De Loe 1995; Clayton 1997). The researcher successfully invited 8 computer forensic experts to participate in the Australian Delphi survey. The issue of the number of Delphi panellists is discussed further in Section 3.5.7. These 8 experts come from different backgrounds but all are experienced in computer forensics. Five of them are academic researchers with long-term industry experience and well-developed collaboration, and the remaining three experts, who work either in a law enforcement agency or a private company, are practical computer forensic investigators. Thus, triangulation of data sources has been achieved and, because experts have been recruited to take part in the Delphi survey, then a valid Delphi survey will also be provided. Discussions on these experts are reported in Section 4.2.1.

Instead of listing the Delphi results by rounds, this thesis lists the results of Australian Delphi survey by dimensions in Section 4.2.2, and also shows the cultural interpretations of these Delphi results by dimensions in Section 4.2.3. This is because the purpose of Australian Delphi survey is to show the unique Australian cultural perspectives rather than the process of consensus of each question. In this section, overall interpretations and conclusions of each dimension are provided.

4.2.1 Experts of the Delphi Survey

Since computer forensics is a specialised topic with a limited small expert population, the Australian respondents of the Delphi survey have been chosen carefully to accurately show the range of current roles played by computer forensic experts. In Australia, experts with a computer forensic background normally belong to government bureaus, such as state-level and federal-level law enforcement agencies, universities, and private companies.

Australian respondents with different backgrounds were invited to participate in the Delphi survey. Because there were only a limited numbers of experts available within the field of computer forensics, then it was only possible to invite eight experts to join this Delphi survey. Based on the discussion in Section 3.5.7 (Clayton 1997; Fitch *et al* 2001), the number, *eight*, not only meets the requirements of a Delphi survey, but also is large enough to meaningfully represent the current research and operational context of computer forensics in Australia. In this thesis, research subjects are introduced anonymously. The first five respondents are academic researchers from different universities, and the other three respondents are practical computer forensic investigators.

4.2.2 Findings of Delphi Survey

The Round One Delphi questionnaire contains 40 different questions, and can be found in Appendix 1. These 40 different questions are classified into 11 sections, which are further categorized into 5 dimensions. The five dimensions are: ***Current Situation Dimension***, ***Policy and Organization Dimension***, ***Education Dimension***, ***Law Dimension***, and ***Personal Preferences and Skills Dimension***.

All Australian Delphi respondents completed the entire Delphi process, which included two rounds of survey. In this thesis, 70% is used as the criterion to decide the accomplishment of Delphi consensus. This indicates that six experts need to have similar opinions in order to reach the consensus for a Delphi question. Under these conditions, there were 10 questions that did not reach consensus in the Round One Delphi survey. Thus, the feedback of these 10 questions was managed, and was used to form the Round Two Delphi questionnaire, which is listed in the Appendix 2. Every question in the Round Two Delphi questionnaire reached the consensus, and no further (Round Three) Delphi questionnaire is needed.

In the following 5 sections (from Section 4.2.2.1 to Section 4.2.2.5), this thesis reports on the Delphi findings based on the order of 5 dimensions rather than the sequence of 40 questions in the Round One Delphi questionnaire. The reason for reporting in this way is that the sequence of the sub-sections is listed randomly so as to prevent participants trying to guess the answers which are desired by the researcher.

4.2.2.1 Current Situation Dimension

The Current Situation Dimension contains Section 1, 2, 3, and 8. There are 17 different questions in total. Question 3, 7, 8, and 28 did not reach consensus, and became Question 1, 2, 3, and 6 in the Round Two Delphi questionnaire. Table 8 shows the consensus and agreement of these Delphi questions, and further points out the relationship between the questions, which did not reach Delphi consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 8: Condition of Consensus and Agreement of Each Question within Current Situation Dimension

	Consensus	Agreement (%)
Round 1, Question 1	Y	75%
Round 1, Question 2	Y	75%
Round 1, Question 3	**N**	**N/A**
=>Round 2, Question 1	**Y**	**87.5%**
Round 1, Question 4	Y	75%
Round 1, Question 5	Y	87.5%
Round 1, Question 6	Y	87.5%
Round 1, Question 7	**N**	**N/A**
=>Round 2, Question 2	**Y**	**87.5%**
Round 1, Question 8	**N**	**N/A**
=>Round 2, Question 3	**Y**	**87.5%**
Round 1, Question 9	Y	87.5%
Round 1, Question 10	Y	75%
Round 1, Question 11	Y	75%
Round 1, Question 12	Y	75%
Round 1, Question 27	Y	75%
Round 1, Question 28	**N**	**50%**
=>Round 2, Question 6	**Y**	**75%**
Round 1, Question 29	Y	87.5%
Round 1, Question 30	Y	75%
Round 1, Question 31	Y	87.5%

4.2.2.2 Policy and Organization Dimension

The Policy and Organization Dimension contains Section 4, and 9. There are 7 different questions in total. Question 13 was the only question which did not reach the requirement of consensus, and became Questions 4 in the Round Two Delphi questionnaire. Table 9 shows the agreement condition of the questions which reached the consensus, and also lists the relationship between questions, which did not reach the

consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 9: Condition of Consensus and Agreement of Each Question within Policy and Organization Dimension

	Consensus	Agreement (%)
Round 1, Question 13	**N**	**37.5%**
=>Round 2, Question 4	**Y**	**87.5%**
Round 1, Question 14	Y	75%
Round 1, Question 15	Y	75%
Round 1, Question 16	Y	75%
Round 1, Question 32	Y	75%
Round 1, Question 33	Y	87.5%
Round 1, Question 34	Y	87.5%

4.2.2.3 Education Dimension

The Education Dimension contains Section 5, and 6. There are 7 different questions in this dimension. Question 23 did not reach Delphi consensus, and became Question 5 in the Round Two Delphi questionnaire. Table 10 shows the agreement condition of the questions which reached the consensus. In addition, Table 10 also lists the relationship between the questions, which did not reach the consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 10: Condition of Consensus and Agreement of Each Question within Education Dimension

	Consensus	Agreement (%)
Round 1, Question 17	Y	87.5%
Round 1, Question 18	Y	75%
Round 1, Question 19	Y	75%
Round 1, Question 20	Y	75%
Round 1, Question 21	Y	75%
Round 1, Question 22	Y	75%
Round 1, Question 23	**N**	**N/A**
=>Round 2, Question 5	**Y**	**87.5%**

4.2.2.4 Law Dimension

There are 4 different questions in this dimension. Question 35 and 37 did not reach the requirement of Delphi consensus, and became Questions 7 and 8 in the Round Two Delphi questionnaire. Table 11 shows the agreement condition of the questions which reached the consensus, and lists the relationship between questions, which did not reach the Delphi consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 11: Condition of Consensus and Agreement of Each Question within Law Dimension

	Consensus	Agreement (%)
Round 1, Question 35	**N**	**37.5%**
=>Round 2, Question 7	**Y**	**75%**
Round 1, Question 36	Y	75%
Round 1, Question 37	**N**	**50%**
=>Round 2, Question 8	**Y**	**75%**
Round 1, Question 38	Y	75%

4.2.2.5 Personal Preferences and Skills Dimension

The Personal Preferences and Skills Dimension contains Section 7, and Section 11, and has 5 different questions. Question 39 and 40 did not reach Delphi consensus, and became Questions 9 and 10 in the Round Two Delphi questionnaire. Table 12 not only shows the consensus and agreement of Delphi questions, but also points out the relationship between questions, which did not reach Delphi consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 12: Condition of Consensus and Agreement of Each Question within Personal Preferences and Skills Dimension

	Consensus	Agreement (%)
Round 1, Question 24	Y	100%
Round 1, Question 25	Y	87.5%
Round 1, Question 26	Y	75%
Round 1, Question 39	**N**	**50%**
=>Round 2, Question 9	**Y**	**75%**
Round 1, Question 40	**N**	**50%**
=>Round 2, Question 10	**Y**	**75%**

4.2.3 Interpretations of Delphi Results

Eight Delphi respondents provided their professional opinions based on their theoretical and practical experience. In this section, the researcher interprets the Delphi consensus from cultural perspectives. These interpretations are based on the five dimensions which were first created in this thesis, so as to simplify and clarify the effect of culture on computer forensic conditions.

Three standpoints need to be explained clearly before introducing the interpretations of Delphi results. The first standpoint is that the questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire are discussed and regarded as a whole. For example, Question 3 in the Round One Delphi questionnaire and Question 1 in the Round Two Delphi questionnaire are considered a single concept. This is reasonable since Question 1 in the Round Two Delphi

questionnaire actually seeks consensus for Question 3 in the Round One Delphi questionnaire.

In addition, the second standpoint is that some Delphi questions (e.g. Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31) only have acultural rather than cultural explanations. This phenomenon is mainly cause by the following reason. The core concepts of these questions are global and independent values which are beyond the cultural influence. Thus, there is no cultural explanation for these Delphi questions.

Lastly, the third standpoint is that certain questions (e.g. Question 11 and Question 23) can only be perfectly explained with the mergence of Australian feedback and Taiwanese findings. Combining the Australian and Taiwanese findings of Question 11 (or Question 23) is able to distinguish the different attitudes in Australian and Taiwanese cultures. In short, there are reasonable cultural explanations for most questions. On the other hand, some questions (e.g. Question 11 and Question 23) are unexplainable unless they are combined with the answers provided by Taiwanese respondents, and others (e.g. Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31) are beyond the influence of different cultures.

4.2.3.1 Current Situation Dimension

There are 17 questions in this dimension, and they are: Question 1 to 12, and 27 to 31. Most of these questions reached consensus except Question 3, 7, 8, and 28. These four questions became Question 1, 2, 3, and 6 in the Round Two Delphi questionnaire respectively. Moreover, these four questions in the Round Two Delphi questionnaire reached 87.5%, 87.5%, 87.5%, and 75% agreement correspondingly. In summary, 17 questions in this dimension reached consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed as follows.

- ***Question 1: From your point of view, what is your government's perspective on computer forensic issues? Do you think the emphasis they put on it is currently at an appropriate level?***
- ***Question 2: What is your opinion on the current developments within computer forensics? Are you satisfied with the current developments of***

computer forensics? Why?

- ***Question 3: How many years has computer forensics existed as a discipline in your country?***
    - ***Derivative Question (Question 1 in the Round Two Delphi Questionnaire): In Australia, the development of computer forensics started around 8-10 years ago. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 4: Is computer forensics a topical issue in your country?***
- ***Question 5: From your viewpoint, what Standard Operation Procedures (SOPs) are used to perform computer forensic investigations in your country?***
- ***Question 6: What is your opinion on the importance of SOPs within computer forensic investigations?***
- ***Question 7: Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?***
    - ***Derivative Question (Question 2 in the Round Two Delphi Questionnaire): Regulations may vary from state to state (from jurisdiction to jurisdiction), but there are regulations that define the time period to keep digital evidence after a trial. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 8: Based on your knowledge, what are the main characteristics of digital evidence? (e.g. Integrity)***
    - ***Derivative Question (Question 3 in the Round Two Delphi Questionnaire): Do you agree with the characteristics of digital evidence within the following table? According to the table, the characteristics can be classified into 15 different categories. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 9: What is your opinion on meta-data of digital evidence from computer forensic perspective?***
- ***Question 10: What is your opinion on the trustworthiness of meta-data of digital evidence?***
- ***Question 11: How would you describe the relationship between computer***

security and computer forensics?

- ***Question 12: When performing a computer forensic investigation, is it necessary to understand the background of the investigated person? (How many dogs they have? What cars they drive? Do they have any habit?) or just focus on analysing the digital data? Why?***
- ***Question 27: Based on your knowledge, have computer forensic investigations in your country ever encountered problems which are caused by time-stamps? or by different time zones? If "YES" how you deal this type of problems?***
- ***Question 28: Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%***
    - ***Derivative Question (Question 6 in the Round Two Delphi Questionnaire): In Australia, 0%-20% of computer forensic investigations encounter encrypted data. At most, 40% of computer forensic investigations encounter encrypted data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 29: Based on your knowledge, how do computer forensic investigators deal with encrypted data in your country?***
- ***Question 30: Based on your knowledge, has performing computer forensic investigations in your country suffered any major difficulties? Can you briefly list them?***
- ***Question 31: "Technical Issues" and "Human Issues" are two separate things. It is easy to examine misuse of a computer, but how to prove the suspect is the one who actually caused this misuse is not an easy task. Based on your knowledge, how do computer forensic investigators deal with this problem in your country?***

In Question 1, six Delphi experts agreed that the Australian government has a proper understanding of computer forensics. This means that 75% agreement was achieved for this question. In addition, these six Delphi respondents consisted of three academic researchers and three computer forensic practitioners.

In Question 2, six Delphi experts agreed that some improvements can be made to the current developments of computer forensics in Australia. These six Delphi respondents consisted of four academic researchers and two computer forensic practitioners.

There was no explicit agreement achieved for Question 3, and the findings of Question 3 can be mainly classified into six categories. Delphi respondents provided various opinions for this question. Therefore, Question 1 in the Round Two Delphi questionnaire was created to seek for the Delphi consensus, and 87.5% agreement was achieved for this question. The consensus shows that seven Delphi experts agreed that forensics has existed as a discipline for 8 to 10 years ago.

Cultural explanations can be provided for the findings of Question 1, 2, and 3. The Delphi consensus of Question 3 is reasonable since Australia, as part of Western society, has a close relationship with the United States of America, which is one of the countries that has led the growth of computer forensic research and practice. Whilst Hofstede's cultural interpretations (1980) did not include inter-cultural metrics, Horne (1964) and Albinski (2001) have both confirmed the close relationship between Australia and the United States of America. Thus, it is not surprising that the development of computer forensics in Australia is only slightly slower than the development of computer forensics in the United States of America. This is indirectly shown in literature (Scientific Working Group on Digital Evidence 1999). The work of the Scientific Working Group on Digital Evidence (1999) shows that the FBI had already published standards and principles for digital evidence in 1999 (9 years ago at time of writing). This indicates that the FBI commenced relevant research before 1999.

In addition, this issue of time frame can also provide a logical account for Question 1 and Question 2. For Question 1, the cultural explanation is very similar to the one for Question 3. Australia has close relationship with the United States of America and Great Britain (Goldsworthy 2005; McLean 2006), and these two countries both have very good research outcomes within the field of computer forensics. The relationship between Australia and Great Britain was confirmed by Horne (1964). This is not surprising since Australia was originally a settled colony of Great Britain. Therefore, it is understandable that the Australian government has a reasonable understanding of computer forensics. In addition, since the development of computer forensics is

continuous in the United States of America or Great Britain, it is reasonable to conclude that the development of computer forensics in Australia would increase at the same rate.

In Question 4, six Delphi respondents, including three academic researchers and three computer forensic practitioners, stated that computer forensics is not a topical subject in Australia. In general, the importance of computer forensic depends on the audience. For example, computer forensics is considered a topical subject in academia and law enforcement. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. This situation is understandable, and is very common in the rest of the world. Because of the uniqueness of computer forensics, it is only a topical subject for a small group of people, such as academic researchers and computer forensic investigators. Unlike economics and/or mathematics, computer forensics draws a small group with a narrow field of expertise. In short, it is understandable that Delphi respondents agreed that computer forensics is not a topical issue in Australia.

In Question 5, seven Delphi respondents, including four academic researchers and three computer forensic practitioners, agreed that there are different SOPs for different organizations. In addition, four of them also stated that there are no national SOPs. The other expert, who works as an academic researcher, expressed that he is not familiar with issues of SOPs since he is not a practical investigator.

In Question 6, most (seven of out eight) Delphi respondents agreed that the value of SOPs is a very important concept within the field of computer forensics. The only Delphi expert with a different opinion stated that it is more important to have standards for competencies, and for tool validation and verification than to have national SOPs. However, having weighed up his opinion, the researcher believes that he is not denying the importance of SOPs. What he actually claimed is that standards for competencies and for tool validation and verification are more important than national SOPs.

There was no clear agreement for the Question 7 of the Round One Delphi questionnaire. Thus, Question 2 of the Round Two Delphi questionnaire was created to seek further Delphi consensus. 87.5% agreement was achieved for Question 2 of the Round Two Delphi questionnaire. The only academic researcher, who did not confirm this question, stated that he is not familiar with the content of this question.

Question 5, 6, and 7 can be explained together by a typical Australian cultural attitude. First of all, the findings of Question 6 need to be interpreted. Most (seven of out eight) Delphi respondents agreed that the value of a SOPs is a very important concept within the field of computer forensics. In addition, they further mentioned that having a computer forensic SOPs is helpful to ensure the integrity and robustness of digital evidence. In this case, computer forensic SOPs can prevent any possible dispute when presenting digital evidence in a court of law. This infers that they realize that SOPs are not only very important for technical purposes, but also significant for legal purposes. In summary, the need for a computer forensic SOPs is the fundamental consensus and global value for computer forensic workers despite their nationalities. Moreover, this concept led to a cultural interpretation for Question 5. Combining the findings of Question 5 and the results of Question 6 shows that science plays an important role in Australian culture. This standpoint can also be found in Slay's work (Slay 2000b). She discussed conceptualisations of nature between Australia and Mainland China, and discussed a Western world view scientifically. Her interpretation of Western world view shows that the value of science is respected in Australian culture. Thus, it is not surprising that different organizations have varied and differing computer forensic SOPs. The previous account explains the existence of different SOPs.

In addition, this cultural attitude can also explain the Delphi consensus of Question 7 (Question 2 of the Round Two Delphi questionnaire). Delphi experts agreed that there are certain regulations that define the time period to keep digital evidence after the trial. This responds to the cultural explanation for Question 5. Australian culture not only focuses on the theoretical issues (e.g. scientific research), but also concentrates on the implementation. The findings of Question 7 also indicate that different states may have different regulations and legislation. This is because the nature of Australian culture values the concepts of independence and autonomy and therefore allows different bodies to take on different responsibilities. This can explain why legislation may differ from state to state. In addition, the explanation for Delphi Question 7 also matches the discoveries of Hofstede's cultural interpretations (1980). According to Hofstede, Australian culture believes in individualism rather than collectivism, and has a small power distance. Thus, Australian culture values autonomy and independence, and considers hierarchy a method for better management. The characteristics of Australian culture mentioned by Hofstede support the cultural interpretations of Delphi Question 7 in this thesis.

There is no clear agreement for the Question 8 of the Round One Delphi questionnaire. Delphi respondents viewed the characteristics of digital evidence from different perspectives and proposed many different opinions. Therefore, Question 3 of the Round Two Delphi question was created to seek further Delphi consensus, and 87.5% agreement was achieved for this question. The only computer forensic practitioner, who did not confirm this question, misunderstood the meaning of this question. In summary, the Delphi respondents stated the characteristics of digital evidence are: maintaining chain of evidence, integrity, electronic form, reliable, and accurate.

The findings of this question show that different cultures do not affect the core scientific values and nature of computer forensics. Two reasons can be provided for this phenomenon. The first reason is that the findings of this question are drawing on essential knowledge of digital evidence. This situation is the same as the addition function in the field of mathematics. In spite of the different cultures from which mathematicians come, the result of one plus one is not going to be affected by culture, and is always two. Moreover, the second reason is that computer forensic experts must have basic computer knowledge, and usually have adequate understanding of computer security issues. The way they learn the essential knowledge of computer is very similar. Thus, it is understandable that they proposed similar characteristic for digital evidence despite their nationalities and cultural backgrounds.

In Question 9, the importance of meta-data of digital evidence was admitted by seven Delphi respondents, including four academic researchers and three computer forensic practitioners. This means 87.5% agreement was achieved for this question. The only academic researcher, who did not confirm this question, stated that he does not have an opinion on this question. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. The importance of meta-data of digital evidence is a fundamental understanding within the field of computer forensics, and this is not affected by the different culture.

In Question 10, six Delphi experts, including four academic researchers and two computer forensic practitioners, stated that the trustworthiness of meta-data of digital evidence is not a serious problem. In general, the meta-data of digital evidence is trustworthy since meta-data of digital evidence is considered another type of digital evidence. If the digital evidence is reliable, the meta-data of digital evidence should be

considered reliable as well. This phenomenon is believed to be affected by the tolerance and acceptance of Australian culture, and is indirectly corroborated by the findings of Question 35. In Australia, members of a court have no problem with the weighting of digital evidence. This infers that they have no problem with the meta-data of digital evidence, which is considered another type of digital evidence. In short, it is understandable that Delphi respondents agreed that the trustworthiness of meta-data of digital evidence is not a problem. In addition, the findings of this question corroborate the concept of Hofstede's cultural interpretations (1980). Hofstede discussed that Australian culture has a weak uncertainty avoidance. This infers that the dissent and the risk are accepted in Australian culture, and further responds to the cultural interpretations of this question. Hofstede's work is consistent with the outcomes of the outcome of this question.

75% agreement was reached for Question 11. This means six Delphi respondents agreed that computer security and computer forensics are two completely different disciplines. The purpose of computer security is to prevent digital incidents from occurring, and the aim of computer forensics is to preserve the outcomes of a digital incident. On the contrary, only two Delphi experts, including one academic researcher and one computer forensic practitioner, stated that these two disciplines have connections. For example, a good understanding of computer security leads to sound computer forensics. The findings of this question are understandable since Australian culture respects individualism, autonomy, and responsibility. This statement is corroborated by concepts from Hofstede's work (1980). Hofstede agreed that the individualism is a major belief in Australian culture and therefore independence and autonomy are two important factors to these people. Not surprisingly, although computer security and computer forensics are analogous subjects, they essentially deal with different digital incidents and have different purposes. Computer security is focused on the prevention of a digital incident, and computer forensics concentrates on preservation of outcomes of a digital incident. Thus, this explanation provides a good reason why computer security and computer forensics are considered two separated subjects.

75% agreement was reached for the Question 12. Five academic researchers and one computer forensic practitioner believed that it is necessary to understand the background of the investigated person in a computer forensic investigation. One out of the other two computer forensic practitioners stated that focusing only on digital

evidence in a computer forensic investigation is enough for most conditions. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. In fact, it is a common technique to use any possible data source to prove the guilt or innocence of the suspect. This means that physical evidence, digital evidence, and any related information are usually required for a legal case. Therefore, it is not surprising that the Delphi consensus of this question occurred.

In Question 27, six Delphi respondents agreed that time issues, which are caused by time-stamps and/or different time zones, are problems for a computer forensic investigation in Australia. On the contrary, one out of the other two Delphi experts, who works as computer forensic practitioner, stated that time issues are not problems within the field of computer forensics. The other expert said that he is not familiar with this issue. This phenomenon can be explained by the following reason. In Australia, there are different time zones and daylight saving times. These two factors deeply affect Australian living styles. People in Australia have to adjust their watches not only for different time zones, but also for the beginning and ending of daylight saving time. Thus, it is reasonable and natural for computer forensic investigators to be concerned over the time issues.

In Question 28, only four Delphi experts believed that a computer forensic investigation reasonable encounters 0%-20% encrypted data. Only 50% agreement was reached, and Delphi consensus was not achieved. Therefore, Question 6 of the Round Two Delphi questionnaire was created to seek Delphi consensus. 75% agreement was achieved for Question 6 of the Round Two Delphi questionnaire. This means that there were six Delphi experts who agreed that a computer forensic investigation reasonable encounters 0%-20% encrypted data (except two academic researchers). This is explainable because Australian living style is relaxed and comfortable (Horne 1964). There is not as great a deal of pressure on basic resources as in Asia and the pressure of life is not so great and its pace not as hectic as in Asia. Thus, Australian culture does not concentrate on competition, and does not place a high level of attention on prevention and protection from crime as in Asia. In short, it is logical that a computer forensic investigation in Australia reasonable encounters 0%-20% encrypted data.

87.5% agreement was achieved for Question 29. Seven Delphi respondents provided several methods (e.g. password cracking and brute force decryption) for dealing with encrypted data. In short, the core concept of these methods is to decrypt the encrypted data. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. Within the field of science, these decryption methods are considered technical skills, and are not affected by different cultures. It is common to use decryption tools for encrypted data. Similar situation can be illustrated by giving the following example. Different cultures cannot affect the basic scientific knowledge. Culture may be able to affect the way people learn addition function, but it cannot affect the result of one plus one. In short, decryption is a rational method to deal with encrypted data, and the attitude of using decryption tools is not affected by different cultures.

In Question 30, six Delphi experts stated that performing computer forensic investigations encounters some difficulties, and these difficulties mainly include lack of manpower, and lack of equipment. This means that 75% agreement was achieved for this question. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. The difficulties, encountered by Australian computer forensic investigators, are actually very common in the rest of the world. It is impossible for the Australian government to put unlimited resources (e.g. money) into the development of computer forensics. In reality, budget is always limited. There is always a lack of money to purchase the latest computer forensic equipments, to recruit more employees, and to set up educational courses. Therefore, it is explainable that these difficulties are cross-national issues, and are very common phenomena in the field of computer forensics.

In Question 31, seven Delphi experts agreed that proving the relationship between the suspect and the misuse of a computer is an important issue within the field of computer forensics. They also stated that collecting as much related evidence as possible is the well-accepted method to build this relationship. The related evidence may include surveillance evidence and fingerprints. The findings of this question show some values within the field of computer forensics that are beyond the influence of culture. In a legal case, using multiple data sources, such as surveillance cameras and fingerprints, to build the link between the suspect and the misuse of a computer is very widespread. Using

other methods is a universal skill to prove the guilt or the innocence of the suspect, and this is not going to be affected by different cultures.

4.2.3.2 Policy and Organization Dimension

Question 13 to 16, 32, 33, and 34 were designed for this dimension in the Round One Delphi questionnaire. Every question reached the Delphi consensus except Question 13, which became Question 4 in the Round Two Delphi questionnaire. In addition, Question 4 in the Round Two Delphi questionnaire reached the 87.5% agreement. In summary, seven questions in this dimension reached the Delphi consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed as follows.

- ***Question 13: In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?***
    - ***Derivative Question (Question 4 in the Round Two Delphi Questionnaire): Not every police station has an electronic crime section. Only federal-level police (e.g. Australian Federal Police (AFP)) and state-level police (e.g. South Australian Police (SAPOL)) have electronic crime section. Thus, the status of computer forensic organization in law enforcement is higher than general police duties. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 14: In your country, do law enforcement organizations out-source computer forensic problems?***
- ***Question 15: Does the organization/department/agency you work for have policies for computer forensic readiness? If "YES", can you provide the name of your organization/department/agency? could you please briefly explain the policies.***
- ***Question 16: In your country, are computer security issues and computer forensics issues dealt by different organization/department/agency? If "YES", how would you describe the relationship between computer security***

organization/department/agency and computer forensic organization/department/agency?

- ***Question 32: Based on your knowledge, have computer forensic organizations/departments/agencies in your country ever had interactions with international organizations/departments/agencies related to similar area? If "YES", how do they interact with other organizations/departments/agencies in other countries?***
- ***Question 33: Based on your knowledge, in your country have computer forensic educational researchers ever had interactions with private/government computer forensic organizations/departments/agencies? If "YES", how do they interact with each other?***
- ***Question 34: Based on your knowledge, employees in the field of computer forensics normally interact or share their professional experiences with (1)colleagues (2)supervisor (3)others (please explain)***

In Question 13, only three Delphi respondents agreed that the status of computer forensic organizations in law enforcement is higher than the status of general police duties. This indicates that the Delphi consensus of this question was not reached. Thus, Question 4 of the Round Two Delphi questionnaire was created to further seek the Delphi consensus. 87.5% agreement was achieved for Question 4 of the Round Two Delphi questionnaire. Only one computer forensic practitioner did not agree with this question because the meaning of the question confused him. This phenomenon can be explained by understanding the nature of Australia culture. The classification of jurisdiction can explain the hierarchical establishment of computer forensic organizations. Since Australia is a geographically large country, hierarchical establishment of computer forensic organizations is necessary and helpful for the convenient implementation. Otherwise, every local police station might need to have its own electronic crime section. This is obviously impossible for the monetary reason. This explanation is also supported by the work of Hofstede (1980). Since Australia has small power distance, the hierarchy is only established for the better management rather than because of the inequality of roles. Hofstede's opinion infers that the hierarchy is helpful for defining the different responsibilities and jurisdictions. In summary, every organization has its own jurisdiction and responsibility, and it follows the hierarchical design so as to maintain the better performance of the system.

In Question 14, six Delphi respondents agreed that law enforcement organizations do not out-source computer forensic problems. The other two Delphi experts with different opinions are both academic researchers. This infers that all computer forensic practitioners agreed that it is not an acceptable way for law enforcement agencies to out-source computer forensic problems. This situation is very likely to be caused by two reasons, which consists of one cultural explanation and one acultural explanation. The cultural reason is that the classification of jurisdiction is very unambiguous and respected in Australia. This means that an expert in law enforcement is only expected to concentrate on his field of expertise. Thus, it is understandable for law enforcement agencies to manage criminal cases which contain computer forensic issues, and for private companies (e.g. accounting company) to only handle civil cases which include computer forensic problems. This standpoint also relates closely to Hofstede's findings (1980). According to Hofstede, individualism is a very important value in Australian culture. It is unsurprising then that autonomy and independence are respected in Australian culture. In addition, the cultural reason is satisfied by the nature of digital evidence. Since digital evidence is eventually going to be presented in a court, it is understandable that law enforcement agencies should be the only organizations that can process digital evidence. After all, the validity and reliability of digital evidence are of most concern when it is presented in a court of law.

In Question 15, 75% agreement was achieved. This indicates that six Delphi respondents agreed that there is no computer forensic readiness in their organizations. These six Delphi respondents consisted of four academic researchers and two computer forensic practitioners. The Delphi consensus shows that computer forensic readiness is rarely found in the Delphi respondents' organizations. The researcher believes this situation is caused by the non-competitive attitude of Australians (Horne 1964). In general, resources are freely available to the population, and this makes Australian living style relaxed and comfortable. Thus, people in Australia sometimes do not think that protection is important and necessary. In this case, although the government, relevant computer forensic organizations, and computer forensic experts realize the importance of computer forensics, they, based on their nature, do not think there is an urgent need for computer forensic readiness.

75% agreement was achieved for Question 16. Six Delphi respondents, including four academic researchers and two computer forensic practitioners, agreed that computer

security issues and computer forensic issues are dealt with by different organizations. The findings of this question can be combined with the results of Question 11 of the Round One Delphi questionnaire, and the new discoveries can be further discussed. According to the Delphi consensus of Question 11, computer security and computer forensics are considered two different topics in Australia. Thus, it is not surprising that the Delphi consensus of Question 16 shows that computer security agency and computer forensic section are two completely different organizations with different capabilities and purposes. This is because Australian culture respects the uniqueness of jurisdiction and responsibility. Since computer security and computer forensics are two different topics, it is reasonable for them to be dealt by different organizations. This cultural interpretation is also borne out by Hofstede (1980), which is discussed in Delphi Question 11. Independence and autonomy are respected in Australian culture. Given that the same underlying cultural differences are proposed, the links to existing literature are the same.

75% agreement was achieved for Question 32. Six Delphi respondents agreed that there are interactions between local computer forensic organizations and foreign computer forensic organizations. There are two Delphi respondents who have different opinions on this question. One expert, who works as academic researcher, was not completely sure about this issue, and the other computer forensic practitioner, who works for a state-level computer forensic organization, stated that there is no international interaction for the state-level computer forensic organizations.

87.5% agreement was achieved for Question 33. Seven Delphi respondents agreed that there are interactions between local computer forensic organizations/workers and local computer forensic organizations/workers. In here, computer forensic workers include academic researchers and computer forensic practitioners. The other expert claimed that he is not familiar with this issue.

Question 32 and Question 33 can be explained jointly, since they have similar cultural explanations. In Australia, electronic crime sections only exist within the federal-level police and state-level police headquarters (e.g. AFP and SAPOL). There is no electronic crime section in the local police station located in a small town. In addition, SAPOL does not have relationship with international computer forensic organizations. On the other hand, the AFP has this type of interactions with other international organizations.

This is comprehensible since SAPOL is state-level police, and its primary task is to manage any criminal case within South Australia. International cooperation and interactions are the tasks belong to the AFP. SAPOL has its own way to conduct interstate interactions. For example, SAPOL cooperates with University of South Australia (UniSA) in computer forensic research. The above phenomena can be explained by the different acknowledgements of jurisdictions and responsibilities. Australian culture realizes and respects that different organizations should have different responsibilities. The AFP and SAPOL are good examples. This discovery responds to the Delphi outcomes of Question 32 and Question 33. In addition, this cultural characteristic is also shown in Hofstede's work (1980). Hofstede showed that Australian culture values the independence and autonomy. His standpoint responds to the cultural findings of this question.

87.5% agreement was achieved for Question 34. Except one computer forensic practitioner who stated that this question is unclear, the rest seven Delphi respondents agreed with this question. In addition, five out of seven Delphi experts stated that they share their professional knowledge with their colleagues and supervisors. Based on the Delphi results of this question, it is interesting to find out that a computer forensic worker not only interacts with his or her colleagues, but also interacts with his or her supervisors. This is because Australian culture thinks that the hierarchy is built for convenience, and that supervisors are meant to be accessible. The nature of Australian culture believes people have equal rights, and these are not changed because of different positions. In addition, Hofstede (1980) proposed a very similar concept, stating that Australian culture has a small power distance, and therefore there is no explicit gap between a supervisor and a subordinate. The existence of hierarchy is to facilitate better management. The other possible explanation for this finding is that colleagues and supervisors can actually help to solve the problem more efficiently and effectively. In summary, the distance between supervisors and subordinates is not obvious in Australia. The interpretation of the Delphi survey responses to this question can be confirmed with the supporting literature quoted above.

4.2.3.3 Education Dimension

Seven questions, Question 17, 18, 19, and 20 to 23, were designed for this dimension in the Round One Delphi questionnaire. Only Question 23 did not reach consensus, and

became Question 5 in the Round Two Delphi questionnaire. In addition, Question 5 in the Round Two Delphi questionnaire reached 87.5% agreement. In summary, seven questions in this dimension reached the Delphi consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed below.

- ***Question 17: How are computer forensic experts produced in your country? through what kind of tests? or procedures?***
- ***Question 18: Do you allow computer forensic experts from other countries to work in a similar job in your country?***
- ***Question 19: Does your country have any organization/department/agency for certifying computer forensic experts? If "YES", what are the names of the organizations/departments/agencies? What criteria do they follow?***
- ***Question 20: Is there any government organization/department/agency willing to support the education/training of computer forensic manpower? or to support the research of computer forensics? Can you briefly explain how the government organization/department/agency supports these agencies?***
- ***Question 21: Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this come from programs?***
- ***Question 22: In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?***
- ***Question 23: Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?***
    - ***Derivative Question (Question 5 in the Round Two Delphi Questionnaire): Although there is no clear method to train a computer forensic investigator, it takes around 2 years to train a computer forensic investigator. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***

In Question 17, besides one computer forensic practitioner, the other seven Delphi respondents agreed that there are different ways to produce a computer forensic expert. This means 87.5% agreement was achieved for this question. Four out of seven Delphi

experts stated that on-the-job training is the major method to form computer forensic experts in Australia. Also, their answers infer that there is no standard method for producing computer forensic experts in Australia.

75% agreement was achieved for Question 18. This means that six Delphi experts agreed that foreign computer forensic experts are accepted. However, one of the other two Delphi experts, who works in a law enforcement agency, stated that being Australian citizen is the prerequisite to work in his organization.
In Question 19, six Delphi experts agreed that there is no organization for certifying the qualifications of a computer forensic expert. The six experts consisted of four academic researchers and two computer forensic practitioners.

75% agreement was achieved in Question 20. Six Delphi experts stated that the Australian government is willing to support education and training within the field of computer forensics. The National Institute of Forensic Science (NIFS) is a good example. This phenomenon can be explained by understanding the Australian culture. Australia has close relationship with the United States of America and Great Britain, and they essentially share the same culture and have very similar traditions. This relationship is explained and proved by Horne (1964) and Albinski (2001). In addition, this relationship is mentioned when discussing the cultural interpretations of Delphi Question 1, 2, and 3. The United States of America and Great Britain are two Western countries that have strong research communities in the field of computer forensic research, and in some ways are the most advanced in the world. Australia's traditionally close ties with these countries enable them to more easily obtain the valuable and practical experiences from the United States of America and Great Britain. In this case, this particular experience is able to help Australian government to understand the importance of computer forensics, and to establish long-term plans for the future developments of computer forensics. The establishment of NIFS is a good example and parallels developments in the USA.

The findings of Question 21 show that six experts, including four academic researchers and two computer forensic practitioners, agreed that there is on-the-job training for computer forensic investigators. Besides the cultural explanations which are going to be provided in the paragraph below, two possible reasons for this situation are provided. The first reason is that the universities are not interested in providing computer forensic

courses due to limited number of computer forensic workers. The demands for these courses are not large enough to support the costs of them. The second reason for this situation is that on-the-job training is the most practical way for junior computer forensic investigators to learn the real experience and latest techniques.

In Question 22, six Delphi respondents, including four academic researchers and two computer forensic practitioners, agreed that there are methods to train computer forensic experts. In addition, four of them stated that the majority of training is on-the-job training. The findings also infer that there is no standard training method in Australia at this moment.

Cultural explanations can be provided for the findings of Question 17, 18, 19, 21, and 22. Here, these questions are discussed jointly, since they all have similar cultural explanations. There is no clear method to produce a computer forensic expert, there is no recognised organization to certify the quality of a computer forensic expert, and there is no universal standard to which to train a computer forensic expert. These phenomena can be explained by understanding the nature of Australian culture. Australian culture accepts various opinions, respects diverse expertise, and values empiricism. In the field of computer forensics, people in Australia currently accept the situation with dissimilar methods and solutions. This not only shows their tolerance, but also demonstrates that they place more attention on the expertises and ability of experts. This indicates that computer forensic experts in Australia do not need to have Master or PhD degrees to prove their ability. Expertise and ability is sometimes more important. In addition, no severe problem is found with this current method. This thus makes the current method and solution acceptable in Australia. Lastly, since Australia culture has a strong focus on expertise and empiricism, they normally are not concerned with the nationality of an expert, except law enforcement agencies which are bound by legislation to do so. These standpoints are supported by the discoveries of Hofstede's work (1980). Hofstede stated that Australian culture has weak uncertainty avoidance. This indicates that acceptance of dissent, empiricism, and expertise are characteristics of Australian culture. What is expressed in Hofstede match the findings of Delphi Question 17, 18, 19, 21, and 22. The confirmation from literature helps to validate these outcomes and place them into a broader context.

The findings in Question 23 can be mainly classified into five categories. There is no explicit agreement for this question. Various opinions are found in this question. Thus, Question 5 of the Round Two Delphi survey was created to seek for Delphi consensus. 87.5% agreement was achieved, and the consensus shows seven experts agreed that training a computer forensic investigator takes around 2 years. The phenomenon discovered by this question can be perfectly explained when combining the Australian and Taiwanese findings of this question. Thus, the cultural interpretation is discussed in Section 6.4.

4.2.3.4 Law Dimension

Four questions, Question 35 to 38, were designed for this dimension in the Round One Delphi questionnaire. The agreements of Question 36 and 38 were both 75%. Conversely, Question 35 and 37 did not reach the consensus, and became Question 7 and 8 in the Round Two Delphi questionnaire. In addition, Question 7 and 8 in the Round Two Delphi questionnaire both reached 75% agreement. In summary, four questions in this dimension reached consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed as follows.

- ***Question 35: In your experience, do courts give a high or low weighting to digital evidence in your country?***
    - ***Derivative Question (Question 7 in the Round Two Delphi Questionnaire): In Australia, digital evidence is given a high weighting in court. Moreover, digital evidence is especially valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 36: Do you know of any difficulties caused by using digital evidence in court? If "SO", what has been the major reason for this?***
- ***Question 37: Based on your knowledge, is it the suspect's obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If "YES", Can you provide the name of the law?***
    - ***Derivative Question (Question 8 in the Round Two Delphi Questionnaire): The situation of computer-based legislation may be different from state to state (from jurisdiction to jurisdiction). Some***

legislation (such as the Cybercrime Act, 2001 and Discovery in Common Law) defines the suspect's obligation for providing digital evidence within Australia. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?

- ***Question 38: Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If "SO", does this affect the attitude of computer forensic investigators to perform investigations? If "YES", can you briefly explain?***

In Question 35, three out of eight Delphi respondents agreed that the court gives a high weighting to digital evidence, but this was not enough for Delphi consensus. Thus, Question 7 of the Round Two Delphi questionnaire was created to seek for further Delphi consensus, and 75% agreement was achieved for this question. Besides two Delphi respondents, including one academic researcher and one computer forensic practitioner, the other six Delphi experts agreed that a high weighting is given to digital evidence in the court.

75% agreement was reached for the Question 36. This means that six Delphi experts agreed that there are some difficulties when using digital evidence in a court. For example, the members of the court, such as lawyers and judges, do not entirely understand the technologies drawn on and used within the field of computer forensics.

It seems that the findings of Question 35 conflict with the results of Question 36. In fact, the findings of these two questions can be combined to provide an overall cultural interpretation. Members of the court give a high weighting to digital evidence despite their poor understanding of digital evidence. There are two cultural reasons for this situation, and these two reasons are deeply related to each other. The first reason caused the above situation is the tolerance within Australian culture. Although members of the court do not have in-depth understanding of digital evidence, they still accept digital evidence as eligible and legal evidence. Of course, this is mainly because of the second reason which explains that Australians accept the value of expertise and empiricism. Since digital evidence is provided and proved by computer forensic experts, its credibility and validity are not considered a problem. This is mainly because that Australian culture realizes that different organizations and/or individuals have different responsibilities. It is computer forensic experts' responsibilities to explain the concept

of digital evidence to members of the court. Literature, specifically Hofstede (1980), states that tolerance and expertise are two important characteristics in Australian culture, by stating that Australian culture has weak uncertainty avoidance. According to his explanation, tolerance and the valuing of expertise are two typical behaviours for a weak uncertainty avoidance.

Four Delphi respondents, including two academic researchers and two computer forensic practitioners, agreed with Question 37. However, this means that only 50% agreement, which is not enough for Delphi consensus, was achieved for this question. Therefore, Question 8 of the Round Two Delphi questionnaire was created to seek for the further Delphi consensus, and 75% agreement was achieved for this question. One out of five academic researchers stated that he is unsure of this question, and one out of three computer forensic practitioners stated that he did not understand this question. The rest six Delphi respondents agreed that there are some regulations (e.g. ***Cybercrime/Computer Crime Legislation 2001*** and ***Discovery in Common Law***) which define the suspect's obligation for providing digital evidence in Australia.

These phenomena are understandable by understanding the thinking of Australians, the behaviour of Australians, and the nature of Australian culture. Using penalties and punishment to prevent people from carrying out malicious activities is very common in most situations. However, the concept of Australian common law (Cater 1995; Heilbronn *et al* 2002) chooses to believe that the nature of humanity is virtuous. In Australian common law, the plaintiff and the corresponding defendant are asked but not forced to exchange relevant evidence, including digital evidence, before the actual trial. They have absolute right to decide whether they exchange the evidence or not. In this case, the pre-settlement is possible, since both parties fully understand all the relevant documentation of each other's case. Australian common law encourages peaceful settlement rather than severe punishment. This infers that people in Australia do believe that the nature of humanity is virtuous and 'innocent until proven guilty'.

75% agreement was reached for the Question 38. Six Delphi respondents agreed that development of computer forensic technologies are beyond the scope of the current legislation. In addition, four out of them stated that this situation does not affect the attitudes of computer forensic investigators. The means these four Delphi respondents believed that their jobs are independent of the outside factors. Consequently, the

previous situation, described in Question 38, does not affect their attitudes. This phenomenon is caused by the following reasons. That the development of a technology or an event is beyond the scope of relevant legislation is a common situation in the world. This is because the design of law is not perfect, and the gap has always existed between legislation and reality (Hojring 2002). Thus, it is understandable that the existence of the gap between the development of computer forensic techniques and existing scope of current laws. In addition, the cultural finding of this question is that four Delphi respondents further stated that the attitudes of computer forensic investigators are not affected by the imperfection of legislation. This is because the nature of Australian culture is to have sound faith in individualism and uniqueness. This infers that outside factors rarely affect Australian' thoughts and behaviours, once they have made their decisions. Hofstede (1980) also provided similar discoveries to the findings of this question, stating that Australian culture is individualist and masculine (very strong and determined) in nature. According to this work, autonomy and independence are two major characteristics of Australian culture. In short, the findings of Hofstede's framework are able to support the cultural interpretation of this question.

4.2.3.5 Personal Preferences and Skills Dimension

There are five questions in this dimension, and they are Question 24, 25, 26, 39, and 40 in the Round One Delphi questionnaire. The agreements of Question 24, 25, and 26 were 100%, 87.5%, and 75% respectively. On the contrary, Question 39 and 40 only reached 50% agreement. This means that they did not reach Delphi consensus, and further became Question 9 and 10 in the Round Two Delphi questionnaire. In addition, Question 9 and 10 in the Round Two Delphi questionnaire reached 75% agreement. In short, Delphi consensuses for these five questions were made after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed as follows.

- ***Question 24: What is your opinion concerning the importance of hash functions in the field of computer forensics?***
- ***Question 25: Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?***

- ***Question 26: Based on your knowledge, what are the countermeasures within computer forensics to the collisions of hash functions?***
- ***Question 39: As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?***
    - ***Derivative Question (Question 9 in the Round Two Delphi questionnaire): In Australia, some computer forensic experts do not use data wiping tools in their work for digital data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 40: As a computer forensic professional, do you use any type of encryption tools for the data in your work?***
    - ***Derivative Question (Question 10 in the Round Two Delphi questionnaire): In Australia, some computer forensic experts do not use encryption tools for their work. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***

100% agreement was achieved for Question 24. Eight Delphi respondents all agreed that the hash function is very important within the field of computer forensics. The importance of the hash function is admitted by Delphi experts despite their backgrounds. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. The purpose of a hash function is to ensure the integrity between original copy and image copy. The importance of the integrity of digital evidence is confirmed by Question 8 of the Round One Delphi questionnaire and Question 3 of the Round Two Delphi questionnaire. From a scientific viewpoint, it is necessary to ensure the integrity of digital evidence in the field of computer forensics. Thus, the importance of the hash function is not a debated issue in the field of computer forensics.

87.5% agreement was achieved for Question 25. Only one academic researcher believed that the collisions of hash functions make digital evidence less robust. The other seven Delphi respondents agreed that the collisions of hash functions are negligible since the possibility for the collisions are very low. The findings of this question show two characteristics of Australian culture. The first characteristic is that Australian culture is tolerant of various opinions and behaviours. As long as the existing solution (multiple hash functions) does not jeopardize the computer forensic process, people in Australia

are willing to accept it as a valid solution. In addition, the second characteristic is that Australian culture is not keen to seek for the absolute answer or solution. Again, Hofstede's work (1980) provided similar interpretations of Australian culture to which the outcomes of this question were able to infer. Hofstede stated that Australian culture is willing to accept different opinions due to weak uncertainty avoidance. This standpoint corroborates the cultural explanation of this question. Consequently, it is not surprising that most Delphi respondents claimed that the impact on computer forensics caused by the collisions of hash functions is negligible.

In Question 26, six Delphi experts, including four academic researchers and two computer forensic practitioners, agreed that there are countermeasures to the collisions of hash functions within the field of computer forensics. For example, using multiple hash functions is a well-accepted method. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. Due to the existence of collisions of hash functions, using multiple hash functions is a well-accepted method for ensuring the integrity of digital evidence. There is currently no better solution. From a scientific point of view, the integrity of digital evidence is completely ensured by using multiple hash functions. In conclusion, technical skills or understandings are not affected by different cultures.

There were only four Delphi respondents, including three academic researchers and one computer forensic practitioner, who agreed with Question 39. This means that 50% agreement was achieved for this question, and then Question 9 of the Round Two Delphi questionnaire was created for seeking the further Delphi consensus. 75% agreement was achieved for the Question 9 of the Round Two Delphi questionnaire. The consensus shows that six Delphi experts agreed that some computer forensic experts do not use data wiping tools in their work for digital data.

There were only four Delphi respondents, including two academic researchers and two computer forensic practitioners, who agreed with Question 40. This means that 50% agreement was achieved for this question, and then Question 10 of the Round Two Delphi questionnaire was created for seeking the further Delphi consensus. 75% agreement was achieved for the Question 10 of the Round Two Delphi questionnaire. The consensus shows that six Delphi experts agreed that some computer forensic experts do not use data encryption tools in their work for digital data.

Question 39 and 40 can be discussed together since they are caused by an identical reason. The percentage of those using data wiping tools and data encryption tools within the Australian Delphi respondents is quite low. As computer forensic experts, some of them do agree that the data wiping tools and data encryption tools are not necessary for every computer forensic expert. From the researcher's perspective, this circumstance is deeply affected by their living environments. Australia is a geographically large country with small population. This indicates that, people do not need to fight for the resources, since the accessible resources are much more than population. This standpoint is proved in Delphi Question 28 by understanding Horne's work (1964). In this case, protection may not be the default assumption in their mind. This cultural explanation provides a rational answer for the reason why certain Australian experts do not think data wiping tools and data encryption tools are necessary since they do not naturally see a need for self-protection from others or to hide their own data.

4.2.3.6 Cross Questions

After interpreting 40 Delphi questions, certain interesting phenomena are found. For example, the findings of Question 30, 36, and 38 can support the findings of Question 2. This situation points out that further (cross-questions) explanations can be provided after combining certain Delphi questions. In this case, the validity of these interpretations is improved by these cross-question corroborations. This section lists and discusses these corroborations.

The findings of Question 30, 36, and 38 corroborate the results of Question 2. In Question 30, lack of manpower and resources is the major problem when performing computer forensic investigations. The findings of Question 36 show that members of the court usually do not entirely understand the basic concepts and characteristics of digital evidence. Lastly, the results of Question 38 point out that the development of computer forensic technology is beyond the scope of current legislation. In conclusion, the findings of previous three questions not only support the results of Question 2, but also prove the trustworthiness of the results of Question 2.

The findings of Question 11 can prove the results of Question 16, and vice versa. In Question 11, computer security and computer forensics are considered two different topics, and these two topics are proved to be dealt with by different organizations in

Question 16. These two questions corroborate the fact that Australian culture respects the uniqueness of jurisdiction, authority, and responsibility. It is understandable for them to be dealt by different organizations, since computer security and computer forensics are two different topics.

The findings of Question 21 are able to support the results of Question 22. In Question 21, the existence of on-the-job training within the field of computer forensics is confirmed. In addition, most Delphi respondents in Question 22 further stated that on-the-job training is the major way to train a computer forensic investigator. Combining the results of these two questions not only enhances the trustworthiness of the outcomes, but also shows that on-the-job training is important in the field of computer forensics.

The results of Question 28 and Question 40 both confirm that the nature of Australian culture is relaxed and comfortable. In Australia, people are usually less competitive due to the richness of resources (Horne 1964). This means that they do not need to fight for resources, to protect themselves and their data, since the resources are more than enough for everyone. One possible interpretation is that this situation infers that they may think that protection is sometimes needless. Thus, it is understandable, from this perspective, that the percentage of the usage of encryption tools is not very high in Australia.

Delphi consensus of Question 35 supports the results of Question 10. In Question 35, Delphi consensus shows that a high weighting is usually given to digital evidence. This means that members of the court are willing to trust the digital evidence. In this case, it is not surprising that they believe the trustworthiness of meta-data of digital evidence, since meta-data of digital evidence is considered another type of digital evidence.

The findings of Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31 are beyond the influence of different cultures. The core concepts of these 10 questions are global and independent values, which are not affected by different cultures. Like addition in the field of mathematics, different cultures cannot alter the result of one plus one. In addition, the discoveries of Question 12 further correspond to the results of Question 31, and vice versa. The importance of using multiple methods and/or data sources is

confirmed in these two questions. In conclusion, the Delphi survey in this research finds there are consistent and independent values within the field of computer forensics.

4.2.4 Summary of Section 4.2

Section 4.2 discusses the experts, results, and interpretations of the Australian Delphi survey. In Section 4.2.1, the backgrounds and expertises of Delphi respondents are introduced, and they are introduced anonymously. This not only infers that the answers and opinions provided by them are compelling and trustworthy, but also confirms the confidentiality of the identities of Australian Delphi respondents. In addition, Section 4.2.2 lists the findings of Australian Delphi survey, and these findings are showed by five dimensions. Lastly, the cultural interpretations of the Delphi results are listed in Section 4.2.3, and these cultural interpretations are also presented by five dimensions. In addition, Section 4.2.3.6 further establishes the relationship between different Delphi questions. Sometimes the results of one question are directly or indirectly proved by the outcomes of the other question. For example, the relationship between Question 11 and Question 16 proves the existence of cross-questions relationship.

In short, the findings of Australian Delphi survey and two case study interviews not only respond to the research question of this thesis, but also proves the relationship between culture and applications of computer forensics.

4.3 Case Study

Case study, unlike Delphi method, is allowed to utilize any possible valuable information regardless of the sources. This indicates that the data from websites, newspapers, memorandums, and personal interviews can also become useful and helpful information for providing the background data when conducting a case study. In addition, case study provides a chance for the case study participant to express his or her mind freely. Unlike Delphi method, the aim of case study is to seek in-depth answers from case study participants rather than seeking for consensus. The thorough explanations of the concept of case study can be found in Section 3.6. Five dimensions, created by this thesis, continue to be used as criteria in case study to examine the latest situation of computer forensics in Australia.

This section presents two Australian case studies without revealing the names of the two case study respondents and their organizations. The two case study respondents were told that their opinions will be presented anonymously. In this way, they do not need to worry about the consequences after giving their opinions, and can thus provide their opinions without any concern. In Section 4.3.1, the first Australian case study is introduced, and Section 4.3.2 describes the second Australian case study. In addition, the comparisons of these two Australian case studies are discussed in Section 4.3.3.

4.3.1 First Australian Case Study

A state-level law enforcement agency was chosen as the organization for the first Australian case study. This is because police officers are the ideal candidates for this case study since they are computer forensic practitioners with real world criminal investigation experience. In addition, the quality of the case study questionnaire was discussed in Section 3.6.6.2.

4.3.1.1 Findings of the First Case Study

This section lists the opinions, provided by Australian Case Study Expert (ACSE) 1, for the case study questions. ACSE 1's standpoints for the latest situations of computer forensics are reflected by these opinions. In addition, 13 case study questions are listed by five dimensions created by this thesis. The first four questions (Question 1 to 4) belong to Current Situation Dimension. Question 5 and 6 belong to Policy and Organization Dimension. In Education Dimension, there are three questions, and they are Question 7, 8, and 9. In addition, Law Dimension consists of two questions, which are Question 10 and 11. Lastly, Question 12 and 13 are listed in Personal Preference and Skill Dimension.

4.3.1.1.1 Current Situation Dimension

Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.

ACSE 1: Yes, my organization does have SOPs. Our SOPs was built by referring to other existing standards and guidelines. For example, the guideline provided by SWGDE is one of these standards. Moreover, I, as a police

officer, know the needs for the court. Thus, our SOPs were built in order to satisfy these needs.

Question 2: Generally speaking, there are two means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

ACSE 1: In the most cases, the computers and/or electronic equipments are seized and forwarded to us. We rarely go to the digital crime scene, and seize the computers and/or electronic equipments. This is not a serious problem at present. The court has accepted digital evidence that is provided by our agency.

Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?

ACSE 1: My department has been established since 2003. The manpower was enough at that time. However, we are seeking new employees right now, since the workload is very heavy with the increased usage of electronic equipments.

Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?

ACSE 1: We actually advertise the position that we need. Moreover, another way that I can think of is that the university can help us to select good student. I personally focus more on the ability rather than the educational qualifications of the candidate.

4.3.1.1.2 Policy and Organization Dimension

Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.

ACSE 1: I do not think this is a serious problem, but I do think that additional work needs to be done. For example, the legislation which defines the issues of encrypted data is an urgent need for our agency. At this stage, it is illegal to force suspects to provide passwords for the encrypted data. Unfortunately, this is the current situation in our state.

However, I do not think this situation affects my attitude when I deal with computer forensic issues. For instance, I actively asked the government to provide appropriate legislation for encryption issues. The software (decryption algorithms) is another applicable solution for encrypted data.

Question 6: In your country, what organisations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.

ACSE 1: I am only familiar with the organizations belong to Australian government. For example, state-level law enforcement agencies (e.g. SAPOL), Australian customs, and federal-level law enforcement agency, such as AFP. In addition, there is a standpoint that I want to clarify. In my organization, we do not deal with digital evidence for commercial purposes. Law enforcement agencies only deal with digital evidence within criminal cases.

4.3.1.1.3 Education Dimension

Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?

ACSE 1: I personally did not have problems of prerequisites or qualifications since I became involved in this area around 10 years ago. In addition, I personally think that on-the-job training is one of the most important training methods within the field of computer forensics.

Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?

ACSE 1: We are moving toward national standard, but at this stage the prerequisites and qualifications are negotiable. This is because some people may have excellent skills without graduating from university. Moreover, I think the training has changed since computer forensics is a dynamic subject. For example, the equipment is improving and very different. Thus, the training has to be different as well.

Question 9: In your country, are there any tertiary-level courses that teach computer forensics?

ACSE 1: As far as I know, there are computer forensic courses in UniSA. I know this since I cooperate with some academic researchers working in UniSA.

4.3.1.1.4 Law Dimension

Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?

B) In your own experience, what is the level of legal knowledge that forensic analysts have?

ACSE 1: A) Yes, I believe this is very important. Moreover, I think the understanding of other laws, such as criminal law, is useful as well.

B) In Australian law enforcement agencies, the majority of computer forensic analysts are police officers as well. Thus, they have good

understanding of legal issues since they become police officers first. For example, I have worked as police officer for 29 years, and I do have good understanding of legal issues.

Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?

B) In your own experience, what is the level of computer forensic knowledge that members of the court have?

ACSE 1: A) I do not complete agree with this statement. I think that members of the court only need to comprehend the computer forensic issues rather than having in-depth knowledge about computer forensics. After all, it is computer forensic investigators' job to provide digital evidence to the court.

B) Unfortunately I think the answer of this question is quite low.

4.3.1.1.5 Personal Preference and Skill Dimension

Question 12: As a computer forensic professional, do you use data wiping tools and/or data encryption tools for your data?

ACSE 1: I sometimes use data encryption tools, but in most conditions, I do not use them.

Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?

ACSE 1: Computer forensic investigators are encouraged to upgrade skills. There are several ways to achieve this goal. For example, identification of training and industry short courses. Moreover, they are also encouraged to study

for higher educational degrees. I think that skills and ability are the first concern for a computer forensic investigator.

4.3.1.2 Interpretations of the First Case Study Findings

ACSE 1 offered his valuable professional opinion according to his practical experiences. Unlike Delphi technique, ACSE 1 was able to express his opinions freely without any limitation. Consensus is never a concern for a high quality case study. The major purpose of this case study is to show the uniqueness of the opinions provided by ACSE 1. In this section, the cultural interpretations of these opinions are given. Tentative cultural explanations are provided to describe how people in Australia behave when they deal with applications of computer forensics. Furthermore, the explanations are made based on the five dimensions, which are first created in this thesis, so as to clearly understand the computer forensic situation.

4.3.1.2.1 Current Situation Dimension

There are four questions in total in this dimension, and they are: Question 1, 2, 3, and 4 in the case study questionnaire. These four questions are listed as follows.

- ***Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.***
- ***Question 2: Generally speaking, there are two common means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?***
- ***Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?***
- ***Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?***

The findings of Question 1 show that the SOPs are a very important issue within the field of computer forensics in Australia. Having SOPs for a computer forensic investigation is not a straightforward task. ACSE 1 claimed that SOPs exist in his organization, and also stated that the SOPs were designed by referring to other well-known computer forensic guidelines and/or standards. One of the major purposes of the SOPs is to satisfy the needs of the court. From the perspective of Australian culture, this situation is explainable. Australian culture emphasizes the value of science. This indicates that Australian culture realizes that the scientific research is valuable because of the scientific nature of the results. Thus, the existence of SOPs is understandable. In reality, SOPs are important and helpful in a computer forensic investigation. This perspective is supported by the work of Slay (Slay 2000b), which examined the interpretations of nature between Australia and Mainland China by considering the Western world view and the Chinese world view. This work shows that in the Western world view science is respected, and this is applicable to Australian culture. This interpretation of the Western world view verifies the cultural explanation of this question and is consistent with the findings.

In Question 2, ACSE 1 stated that digital equipment is normally seized and forwarded to his organization in most situations. He further stated that it is currently not a problem for the court to accept digital evidence. This current state can be explained by understanding the nature of Australian culture. Australian culture is more able to accept dissent. This means that tolerance is part of Australian culture. Different situations can exist at the same time, and they are all acceptable. This standpoint is also verified by Hofstede's work (1980). Hofstede used the same concept to interpret the nature of Australian culture because he concluded that Australian culture has weak uncertainty avoidance. In summary, people in Australia accept different situations as long as these situations do not break the laws and/or jeopardize their tasks.

In Question 3, ACSE 1 said the manpower in his organization was sufficient on the establishment of his organization on 2003. However, he admitted that there is currently a shortage of computer forensic employees. Thus, his organization is seeking for new computer forensic employees, since the workload is very heavy with the increased usage of electronic equipments. In summary, ACSE 1 agreed that the manpower is currently not enough for his organizations. This discovery essentially responds to the findings of Delphi Question 30, and shows that some values within the field of

computer forensics are beyond the influence of culture. This situation is practical because the Australian government cannot support computer forensic activities without any restriction (e.g. unlimited budgets). In reality, the Australian government cannot focus only on computer forensic issues, and ignore other serious matters. Consequently, the shortage of computer forensic workers is understandable, and this situation is not obviously affected by a cultural influence.

ACSE 1, in Question 4, stated that advertising is a common way for him to recruit new employees. He further said that university and personal relationships are helpful in finding eligible employees as well. In addition, ACSE 1 stated that he focuses more on the ability rather than the educational qualifications of the candidate. This indicates that people in Australia focus not only on the importance of professional qualifications, but also on the real experiences, the expertises, and the importance of empiricism. When Australians recruit new employees, they concentrate more on the ability of the employee than his or her educational qualifications. This situation also infers that they consider the value of the people rather than the role of the people. In addition, this statement is also confirmed by Hofstede (1980). According to his work, experience, expertise and empiricism are three important factors in Australian culture.

4.3.1.2.2 Policy and Organization Dimension

There are two questions, Question 5 and 6 of the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.***
- ***Question 6: In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.***

In Question 5, ACSE 1 stated that government policies for computer forensics are not perfect, but do not cause too much trouble. For example, he stated that legislation about the encryption issues is an urgent need for his organization. But he also stated that he is not affected by the lack of updated legislation, and chooses to actively ask the

government to legislate against encryption problems. This situation can be explained by the following cultural reasons. Since Australian culture normally focuses on the ability of an individual, it is not surprising that initiative and achievement of an individual are also very significant and valuable in Australian culture. This indicates that performance is an important aspect to measure the effectiveness of an individual. This can explain ACSE 1's active action for legislating against encryption issues. In addition, ACSE 1's opinions show that Australian' thoughts and behaviours are rarely affected by outside factors (e.g. government policies). This is because Australian culture concentrates on individualism and independence. Therefore, people in Australia are independent and autonomous. In addition, according to Hofstede's research (1980), the findings of this question are reasonable. This is because Hofstede provided very similar cultural interpretations for Australian culture as well. He stated that individual initiative and independence are two important features in Australian culture.

In Question 6, ACSE 1 stated that law enforcement agencies (e.g. the AFP and state police agencies) and Australian customs have the ability and the legal function to deal with computer forensic issues. In addition, he also said that digital evidence involved in criminal cases is always dealt with by law enforcement agencies. This situation is comprehensible by understanding the nature of Australian culture. Australian culture respects individualism, and treats every event and every person individually. This indicates there is a clear line for the duties of law enforcement agencies and private companies. Criminal cases are always the responsibilities of law enforcement agencies. In summary, the classification of jurisdiction and responsibility is clearly defined and respected in Australia. Moreover, Hofstede (1980) also described that autonomy and independence are two explicit features in Australian culture.

4.3.1.2.3 Education Dimension

There are three questions, Question 7, 8, and 9 in the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?***

- ***Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?***
- ***Question 9: In your country, are there any tertiary-level courses that teach computer forensics?***

The findings of Question 7 and 8 can be discussed together. ACSE 1 stated that there was no clear rule for technical prerequisites or qualifications for him when he started his current career. In addition, ACSE 1 stated that the national standard for certifying computer forensic experts is going to be established in the near future, but he also thought that technical prerequisites and qualifications for new employees are negotiable. This is mainly because qualifications and practical skills are sometimes not equal to each other. Lastly, he admitted the importance of on-the-job training within the field of computer forensics, and thinks that on-the-job training is one of the most important training methods for computer forensic investigators. In summary, ACSE 1 chooses to believe the technical ability of new employees more than their educational qualifications, and also values the role of on-the-job training within the field of computer forensics. This phenomenon can be explained from the Australian culture perspective. Empiricism is a well-accepted concept in Australian culture. People in Australia normally focus on an individual's ability rather than his or her academic qualifications. Due to this nature, it is understandable that ACSE 1 is more willing to recruit new employees with excellent technical skills but without formal qualifications. In addition, this situation also shows that Australian culture is willing to accept different methods for hiring a computer forensic investigator. Different methods are acceptable, as long as they are reasonable. The findings of this question are supported by the discoveries of Hofstede's work (1980). He expressed that Australian culture emphasizes the empiricism of an individual and is more willing to accept different opinions. The outcome of this question and the underlying reasoning respond to the findings of Hofstede's research, and this helps verify the outcomes and interpretation of this question.

In Question 9, ACSE 1 confirmed that there are computer forensic courses in UniSA, and further stated that he has cooperation with certain academic researchers within UniSA. This situation shows that cooperation between different types of organizations

is treated seriously in Australia. Law enforcement agencies can work together with universities for discovering advanced knowledge and/or obtaining mutual benefits. Although Australian culture focuses on the classification of jurisdiction and exclusive responsibility, this does not stop cross-organizations or cross-disciplines cooperation. The classification of jurisdiction can be found in Hofstede's research (1980) as well. He described that Australian culture emphasizes autonomy and independence. This indicates that the trustworthiness of the findings of this question is not a problem. Within the field of computer forensic, the cooperation between academia and practical organizations, such as law enforcement agencies and accounting companies, is especially important for improving the future development of computer forensics.

4.3.1.2.4 Law Dimension

There are two questions in this dimension, and they are Question 10 and 11 of the case study questionnaire. These two questions are listed as follows.

- ***Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?***

  B) In your own experience, what is the level of legal knowledge that forensic analysts have?
- ***Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?***

  B) In your own experience, what is the level of legal knowledge that members of the court have?

An overall explanation can be provided by combining the findings of Question 10 and 11. In Question 10, ACSE 1 claimed that it is not a problem for him to understand legal issues which are associated with computer forensics. His reasoning for this is that the majority of computer forensic analysts are police officers, and police officers have a good understanding of legal issues, based on their initial and ongoing training. In Question 11, instead of in-depth knowledge of computer forensics, ACSE 1 agreed that members of the court should only need basic understanding of computer forensics.

If this situation is interpreted from cultural perspectives, there are two reasons for this condition. The first cultural reason is that Australian culture respects the value of experience and personal expertise. An individual's expertise is respected because of the nature of Australian culture. The second cultural explanation for the situation is that Australian culture respects the classification of jurisdictions and responsibilities. It is computer forensic experts' responsibility to explain computer forensic issues in a court of law, since members of the court have outstanding legal knowledge rather than computing knowledge. In addition, these two cultural reasons are further corroborated by Hofstede's cultural interpretations (1980). Hofstede's research states that empiricism, autonomy, and independence are major characteristics of Australian culture. In summary, the discoveries of this question can be partially verified, given that there is substantial literature (Hofstede 1980) with an agreement as to the results and cultural underpinnings.

4.3.1.2.5 Personal Preference and Skill Dimension

There are two questions in this dimension, and they are Question 12 and 13 of the case study questionnaire. These two questions are listed as follows.

- ***Question 12: As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?***
- ***Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?***

The findings of Question 12 show that ACSE 1 does not really use data wiping tools and/or data encryption tools although he works as a computer forensic expert. From the researcher's point of view, this condition is explainable from a cultural perspective. Australia is a geographically large country full of nature resources, but only has small population. This standpoint is consistent with the viewpoint expressed by Horne (1964) and is discussed in greater detail in Delphi Question 28. This means people do not need to compete for resources. Thus, Australian living style usually does not force individuals to guard themselves from other people and situation, and life is relaxed and comfortable. The researcher believes this is the major reason for ACSE 1's answer, since he does not think self- protection is necessary (Horne 1964).

Question 13 was asked to find out the how ACSE 1's organization upgrade the technical skills of its computer forensic specialists. The findings show that there is no standard method for this issue. Technical skills are upgraded in several ways, such as attending industry short courses, and obtaining higher educational degrees. In addition, ACSE 1 agreed that the skills and ability of employees are more important than educational qualifications, and he is willing to recruit new staff with excellent technical skills but without formal educational qualifications (e.g. Master degree and PhD degree). He further stated that one of his colleagues is actually studying at UniSA for a higher educational degree right now. Based on his answer, it clearly shows that different methods are acceptable in Australian culture and empiricism is respected in Australian culture. Thus, it is realized that tolerance and empiricism are important parts of the Australian culture. In addition, these two cultural perspectives are consistent with the outcomes of Hofstede (1980). Hofstede stated that Australian culture has weak uncertainty avoidance. The typical characteristics of weak uncertainty avoidance are accepting different opinions, and emphasizing empiricism. In short, the cultural underpinnings of this question may be further enhanced as it is reconcilable with Hofstede's work (1980).

4.3.1.2.6 Cross Questions

Possible relationships between or among case study questions are introduced in this section. Nevertheless, there are some questions that may not be grouped with other questions, as there is no relationship between them. However, Question 4 and 9, Question 4, 8 and 13, and Question 7 and 8 all explore similar themes to each other.

Although the findings of Question 4 do not directly prove the outcomes of Question 9, the discoveries of these two questions show that there is cross-organization cooperation between ACSE 1's organization and UniSA. These discoveries show that ACSE 1 not only believes that the university can help for recruiting future computer forensic employees, but also stated that cooperating with the university is important and useful. In short, the outcomes of Question 4 and 9 show that cross-organization cooperation is an important concept within Australian culture.

Combining the findings of Question 4, 8, and 13 is able to show that the ability of a computer forensic investigator is very important in Australian culture. In case study

Question 4 and 13, ACSE 1 clearly stated that he focuses more on the ability of an employee rather than the his or her educational qualifications. In addition, ACSE 1 gave a similar opinion in Question 8. Although this opinion does not directly respond to the results of Question 4 and 13, this opinion indeed points out that ability of an individual is undoubtedly more important than academic qualifications. The corroboration among the previous three questions is actually achieved by understanding the findings. In short, the outcomes of the previous three questions show that empiricism is considered seriously by Australian culture.

Combining the findings of Question 7 and Question 8 is able to show that empiricism is an explicit feature within Australian culture. In Question 7, ACSE 1 stated that he did not pass any exam for his current position. In addition, the findings of Question 8 point out that there is no related exam for the future employees at present. Combining the results of these two questions shows that empiricism is an important value in Australian culture. The ability of an individual can be considered the most important attribute for the individual.

4.3.2 Second Australian Case Study

The second Australian case study is introduced in this section. The fundamental information for this case study is presented so as to understand the quality of this case study. The information includes the quality of organization, the quality of the case study respondent, and the quality of the case study questionnaire. By understanding these three quality issues, the quality of this case study is proved. These proofs are important since the quality of the case study is a major concern of this thesis.

In this thesis, a private accounting company is the organization for the second Australian case study. In Australian, relevant civil disputes, which include computer forensic problems, can be dealt with by private accounting companies. This situation not only means the private accounting company is suitable for this case study, but also infers that computer forensic practitioners working for these company are appropriate candidates for this case study. Lastly, the quality of the case study questionnaire was discussed in Section 3.6.6.2. In short, the quality of the second Australian case study is confirmed by checking previous three factors.

4.3.2.1 Findings of the Second Case Study

The opinions provided by ACSE 2 are listed in this section. These opinions are able to truly reflect ACSE 2's standpoints for the latest conditions of computer forensics in Australia. Five dimensions created by this thesis are still used to classify the 13 case study questions. The first four questions (Question 1 to 4) belong to Current Situation Dimension. Question 5 and 6 belong to Policy and Organization Dimension. In Education Dimension, there are three questions, and they are Question 7, 8, and 9. In addition, Law Dimension consists of two questions, which are Question 10 and 11. Lastly, Question 12 and 13 are listed in Personal Preference and Skill Dimension.

4.3.2.1.1 Current Situation Dimension

Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.

ACSE 2: Yes, my organization has SOPs for computer forensic purposes. Instead of developing the SOPs in-house, these SOPs adapt other existing standards, such as industry based guidelines. Moreover, the SOPs in my state police E-Crime Lab is one of these standards. In this case, it is easier for my state police to trust the credibility of my reports.

Question 2: Generally speaking, there are two common means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

ACSE 2: I do not think there is a difference between these two collection methods, unless non-technical individuals actually process the seized equipments or data. For example, integrity may become a problem. They probably do not use computer forensic hardware and software, and do not follow the regulations.

Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?

ACSE 2: Not currently. I am looking forward to recruit more people for my department next year.

Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?

ACSE 2: Normally the advertisement is put on the newspaper. Another way is to find people through personal relationship. In addition, my major concern about the new employees is his or her professional ability.

4.3.2.1.2 Policy and Organization Dimension

Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.

ACSE 2: I do not know the current government policy. However, from my perspective, I think the policy and my works are two separate things. I still need to provide the concreteness of digital evidence despite different policies.

Question 6: In your country, what organisations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.

ACSE 2: I think the answers are depending on the different situations. If it is a criminal case, the police are the only choice. On the other hand, if it is a business dispute, I can deal with the problem first, and then send the report to the police.

4.3.2.1.3 Education Dimension

Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?

ACSE 2: I have been a computer forensic investigator for 3.5 years. I personally do not encounter problems, but I think qualifications are useful and helpful.

Yes, on-the-job training is provided in my organization. For example, junior computer forensic investigators can work with senior computer forensic investigators to obtain valuable experience. I think computer forensic investigators are able to obtain most of their experience by proper on-the-job training. Of course, computer forensic investigators are also sent to attend vendor-based courses.

Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?

ACSE 2: I put more emphasis on the ability of the employees. I would accept a person with excellent computer skills, but without qualifications. The qualification is beneficial in some cases, but does not mean everything. It is very easy for a person having computer ability to have formal qualifications. In addition, I think that training change as the techniques change.

Question 9: In your country, are there any tertiary-level courses that teach computer forensics?

ACSE 2: I do not entirely understand the situation, but I think that there are computer forensic courses in UniSA. Due to the uniqueness of computer forensic, the number of computer forensic workers is limited in South

Australia. This indicates that people know each other within this small group. For example, I have good relationship with SAPOL and UniSA.

4.3.2.1.4 Law Dimension

Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?

B) In your own experience, what is the level of legal knowledge that forensic analysts have?

ACSE 2: A) Yes, I believe this is very important, but I do not think the in-depth understanding is necessary.

B). I think that the mutual understanding between computer forensic investigators and members of the court should be enhanced.

Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?

B) In your own experience, what is the level of computer forensic knowledge that members of the court have?

ACSE 2: A) The answer is the same as the previous question. Yes, I believe this is very important, but I think that they only need to have the basic understanding of computer forensic issues and techniques. Members of the court can understand the computer forensic issues through the explanations of computer forensic experts. This is the value of computer forensic experts.

B) The answer is the same as the previous question. I think that the mutual understanding between computer forensic investigators and members of the court should be enhanced.

4.3.2.1.5 Personal Preference and Skill Dimension

Question 12: As a computer forensic professional, do you use data wiping tools and/or data encryption tools for your data?

ACSE 2: I would encrypt some information. However, I do not use data wiping tools. The only exception is that I use data wiping tools when the old hard disk is replaced.

Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?

ACSE 2: Sending computer forensic investigators to vendor-based courses and conferences is the main way to upgrade their skills and knowledge. From my perspective, skills and ability are the most important features for a computer forensic investigator. My company does not rely on in-house courses, since the company is not big enough to have its own computer forensic courses.

4.3.2.2 Interpretations of the Second Case Study Findings

The valuable and professional opinions provided by ACSE 2 are listed in the previous section (Section 4.3.2.1). Unlike Delphi technique, ACSE 2 can express his opinions freely and without any limitation. Consensus is never a concern for a high quality case study. The ultimate aim for this case study is to show the uniqueness of ACSE 2's professional standpoints. In this section, the cultural interpretations of ACSE 2's opinions are given. Based on these cultural interpretations, it is possible to understand how Australians think and behave when they deal with computer forensic issues. Five dimensions are used to classify these cultural interpretations in order to understand the computer forensic conditions straightforwardly.

4.3.2.2.1 Current Situation Dimension

There are four questions in total in this dimension, and they are: Question 1, 2, 3, and 4 in the case study questionnaire. These four questions are listed as follows.

- ***Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.***
- ***Question 2: Generally speaking, there are two common means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?***
- ***Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?***
- ***Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?***

In Question 1, ACSE 2 admitted that the SOPs are a very important issue within the field of computer forensics. Having SOPs for computer forensic investigations is not a straightforward task, but it is essential for a computer forensic investigation. In addition, he claimed that SOPs existed in his organizations, and also stated that the SOPs were designed by referring to other well-known computer forensic guidelines and/or standards. This means that the SOPs were not developed in-house. This is understandable since Australian culture esteems the importance of science. This situation further infers that Australian culture also emphasizes the value of scientific results. The Australian understanding of science was provided by Slay (2000b). The work of Slay corresponds with the fin dings of this question, which helps to affirm the trustworthiness of the cultural interpretation of this outcome.

ACSE 2 did not believe that there is a difference between the two collection methods mentioned in Question 2. As long as the non-technical investigators do not actually process the seized equipments or data, both methods are considered acceptable and legitimate. The findings of this question are not surprising since the nature of Australian culture is a willingness to accept dissent. This situation also shows that tolerance is part of Australian culture. A particular method is not acceptable only if it breaks the laws and/or jeopardizes its original purpose. This viewpoint is consistent with the work of

Hofstede's work (1980). Hofstede also agreed that accepting dissent is a typical attitude of Australian culture.

In Question 3, ACSE 2 admitted that there was a shortage of manpower in his department, and he is seeking new computer forensic workers. Coincidently, his opinion corresponds to the findings of Delphi Question 30, and shows that some values within the field of computer forensics are beyond the influence of culture. This state is reasonable since it is impossible for an accounting company to support computer forensic activities without restrictions. In reality, there are other goals (e.g. annual financial goal) for an accounting company to achieve. Computer forensic issues are not the only concern for an accounting company. Accordingly, the shortage of computer forensic workers is understandable, and culture is not the reason for this circumstance.

In Question 4, ACSE 2 stated that advertising is a common way to recruit new employees, and he also said that personal relationship is helpful for finding eligible employees. In addition, ACSE 2 stated that his major concern about the new employees is his or her professional ability. ACSE 2 puts more emphasis on experiences and expertises than on educational qualifications. This standpoint is understandable since Hofstede's research (1980) shows a similar result. According to Hofstede, experience and empiricism are very important in Australian culture. This work indicates a similar cultural standing, with ASCE2 giving the same message. In short, the finding of this question shows that Australian culture focuses on the real experiences, expertise, and the importance of empiricism, and the finding is trustworthy due to the discoveries of Hofstede's work (1980).

4.3.2.2.2 Policy and Organization Dimension

There are two questions, Question 5 and 6 of the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.***
- ***Question 6: In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government***

departments and private companies.

In Question 5, ACSE 2 stated that government policies and his works are two individual things. His argument proved that his attitudes toward computer forensics are not affected by the development of current government policies. There is a cultural reason for this situation. Australian culture concentrates on individualism and independence. Therefore, people in Australia are confident in their beliefs, standpoints and behaviours. This indicates that their beliefs, standpoints and behaviours can rarely be affected by outside factors. The cultural interpretation that is the outcome of this response is corroborated by Hofstede (1980), as this work stated that autonomy and independence are important parts in Australian culture. Here, the outside factor means government policies. In short, people in Australia are independent and autonomous.

In Question 6, ACSE 2 stated that he can only deal with the business disputes since criminal cases are the responsibility of law enforcement. This situation can be explained by understanding the nature of Australian law and culture. Australian culture respects individualism. This means every event, person, and organization is treated individually. Therefore, there is a clear line between the duties of law enforcement agencies and private companies. The classification of responsibility is clearly defined and respected in Australia. as with the previous question, the trustworthiness of the cultural explanation of this question is proved and enhanced by direct comparison to the work of Hofstede (1980) as these two works are consistent.

4.3.2.2.3 Education Dimension

There are three questions, Question 7, 8, and 9 of the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?***
- ***Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed***

since you undertook them?

- ***Question 9: In your country, are there any tertiary-level courses that teach computer forensics?***

The findings of Question 7 and 8 can be discussed together. ACSE 2 stated that he personally did not encounter problems caused by technical prerequisites or qualifications when he started his current job. In addition, ACSE 2 said that he would put more emphasis on the ability rather than educational qualifications of the new employees, and admitted that the importance of on-the-job training within the field of computer forensics. This phenomenon can be explained and interpreted by Australian culture. Australian culture respects the value of empiricism. An individual's ability usually obtains more attention than his or her academic qualifications. In addition, this situation also shows that different recruiting methods are accepted by Australian culture. This means Australian culture is tolerant of different choices and opinions. As long as these recruiting methods are reasonable, they are considered suitable and acceptable. The previous two cultural explanations are both demonstrated in Hofstede's work (1980). In his work, he shows that empiricism and acceptance of different opinions are two features of Australian culture. By drawing on his cultural interpretations, it is realized that a cultural explanations of this question is trustworthy and appropriate.

In Question 9, ACSE 2 believed that there are computer forensic courses in a local university, and stated that he has good relationship with his state and a local university. This statement points out that cooperation is a very important concept in Australia. This is because Australian culture respects the classification of jurisdiction and exclusive responsibility. This viewpoint is reconcilable with the position used by Hofstede (1980), who stated that Australian culture emphasizes autonomy and independence. Universities, law enforcement agencies, and private companies always focus on different parts of the computer forensic situation. Thus, proper cooperation is the major way to connect two or more individual parties to develop novel and significant knowledge and/or to obtain mutual benefits. Within the field of computer forensics, cooperation between academia and practical organizations, such as law enforcement agencies and accounting companies, is especially important for improving the future development of computer forensics.

4.3.2.2.4 Law Dimension

There are two questions in this dimension, and they are Question 10 and 11 of the case study questionnaire. These two questions are listed as follows.

- ***Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?***

  B) In your own experience, what is the level of legal knowledge that forensic analysts have?
- ***Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?***

  B) In your own experience, what is the level of legal knowledge that members of the court have?

The findings of Question 10 and 11 can be discussed together in order to provide an overall explanation. In Question 10, ACSE 2 believed this understanding is important, but does not think the in-depth understanding is necessary. He further stated that the mutual understanding between computer forensic investigators and members of the court should be enhanced. From his perspective, computer forensic investigators should be more familiar with legal issues. In Question 11, ACSE 2 agreed that the members of the court only need basic understanding of computer forensic issues. In-depth understanding is not necessary. His reasoning for this is that it is computer forensic experts' responsibilities to explain computing issues clearly and thoroughly to the arbitrators of a case.

There are two cultural reasons for the findings of Question 10 and 11. The first cultural reason is that Australian culture respects the value of expertise. This means that an expert may perform well in his of her domain, but does not know in-depth knowledge about other domains. In addition, the second cultural reason is that Australian culture respects the classification of responsibilities. It is computer forensic experts' duty to explain computer forensic issues in a court of law, since the expertise of the members of the court is legal knowledge rather than computing knowledge. The two cultural interpretations for this question are both consistent with the work of Hofstede (1980). This consistency enhances the validity of these outcomes. This is because Hofstede also

believed that Australian culture includes these two cultural characteristics (empiricism and independence).

4.3.2.2.5 Personal Preference and Skill Dimension

There are two questions in this dimension, and they are Question 12 and 13 of the case study questionnaire. These two questions are listed as follows.

- ***Question 12: As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?***
- ***Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?***

In Question 12, ACSE 2 stated that he uses data encryption tools more frequently than data wiping tools. This phenomenon can be explained from a cultural perspective. This viewpoint confirms the perspective of Horne (1964), and is discussed in detail in Delphi Question 28 and indicates that precaution is not an important issue in Australian culture. Thus, it is not surprising that they do not think data encryption and wiping tools are necessary.

In Question 13, ACSE 2 said that there are several ways rather than a standard method to upgrade the technical skills of computer forensic specialists. The major method is sending computer forensic investigators to vendor-based courses and conferences. In addition, ACSE 2 agreed that the ability of an employee is more important than his or her educational qualifications. Thus, he is willing to recruit new staff with excellent technical skills. He further stated that one of his colleagues, who is currently working in Sydney office, is a good example of this standpoint. The colleague started his current job without a university qualification, but he is brilliant with computer forensic techniques. According to ACSE 2's answers, it shows that Australian culture is able to endorse different recruiting methods, and is also able to emphasize the experience of an individual. This indicates that the tolerance and empiricism are two important parts of the Australian culture. In addition, these two concepts are shown to be in keeping with the outcomes of research by Hofstede (1980). He agreed that these two concepts are

parts of the Australian culture. Comparison to this work explicitly enhances the findings of this question.

4.3.2.2.6 Cross Questions

The purpose of this section is to list any possible relationship between or among case study questions. However, some case study questions may not have this type of relationship. After examining 13 case study questions, relationships only exist among Question 4, 8, and 13, and between Question 7 and 8.

In Question 4, 8, and 13, ACSE 2 stated that he concentrates on the technical ability of the future employees rather than their educational qualifications. This demonstrates that the importance of empiricism within Australian culture. In addition, the corroboration among these three questions enhances the trustworthiness of the findings. In summary, empiricism plays an important role in Australian culture.

Combining the discoveries of Question 7 and 8 is able to show the same conclusion as the corroboration proved by the results of Question 4, 8, and 13. The results of these two case study questions reveal that empiricism is an important part within Australian culture. An individual's ability is more attractive than his educational qualifications. The ability of an individual can be considered the most important attribute for the individual.

4.3.3 Comparison of Australian Case Studies

The two Australian case studies do not show identical responses and trends, but they do provide very similar results. This means that ACSE 1 and ACSE 2 have close opinions although they come from two different organizations. In addition, this section uses other types of data sources to demonstrate the trustworthiness of the opinions from two case study participants. The use of other types of information is appropriate since this is the core value of case study research. The detailed discussions of case study can be found in the Section 3.6. However, one standpoint should be explained in order to clarify the concept of this thesis. The multiple data sources for some questions may not be found.

In Question 1, SOPs are carried out in practice. According to the answers of the two case study participants, their organizations both have their own SOPs, and these two different SOPs are built in a similar way, which refers to other existing standards and guidelines. In addition, there are several guidelines or SOPs that can be found within Australian. For example, the Australasian Centre for Computing Research (2003) provides a basic guide called, *Seizing Computers and other Digital evidence*, to help police officers to seize digital evidence. This document provides the basic rules for seizing computers and other electronic devices, and can be considered a type of SOP for Australian police officers. In addition, according to Ghosh (2004), *Guidelines for the Management of IT Evidence* was launched by Standards Australia on 12/08/2003. The guidelines can be considered another Australian SOP as well. Lastly, Beckett and Slay (2007) discussed SOP issue from an academic perspective. They argued issues of the use of SOPs from the concept of validation and verification. In summary, according to the previous data sources, it is realized that the importance of computer forensic SOPs is acknowledged in Australia even though consensus on their nature has not been reached..

In Question 6, ACSE 1 stated that electronic crime sections are existed in the law enforcement agencies (e.g. AFP and SAPOL). It is understandable for law enforcement agencies to have computer forensic departments, since they are the only eligible organizations to provide digital evidence for criminal cases. In addition, according to ACSE 2, accounting companies are able to deal with the civil disputes with computer forensic issues. Besides law enforcement agencies and accounting companies, there are other national organizations which are interested in computer forensic issues. For example, the Australasian Centre for Policing Research (Australasian Centre for Policing Research 2007) which helps to provide the research results for police force in several domains, such as alcohol, electronic crime, drug, gambling, and identity crime. In addition, the NIFS (National Institute of Forensic Science 2007) also places attention on the development of computer forensics. In summary, there are some government organizations, including federal-level and state-level organizations, and private companies interested in the issues of computer forensics.

In Question 9, ACSE 1 and ACSE 2 believed that his local university has computer forensics courses. The responses of ASCE1 and ASCE2 both show that cross-organization cooperation is a very important concept in Australian culture. Nevertheless, his local university is not the only university that provides tertiary-level

computer forensic courses. There are other universities that also provide computer forensic courses and/or conduct academic research in this area. For example, three well-known universities are Deakin University, Edith Cowan University, and Queensland University of Technology. In addition, according to the NIFS (National Institute of Forensic Science 2007), an advanced diploma of computer forensics is provided by Canberra Institute of Technology. In summary, computer forensics is not as popular as computer security, but the development of computer forensics courses is indeed admitted by certain universities and NIFS.

4.3.4 Summary of Section 4.3

There are two Australian case studies presented in Section 4.3. The first Australian case study is introduced in Section 4.3.1, and three quality factors (case study organization, participant, and questionnaire) of this case study are introduced as well. Based on the discussions of the quality factors of the first Australian case study, the quality of the case study findings is ensured. Lastly, these findings are further interpreted from the cultural perspectives in Section 4.3.1.2.

Section 4.3.2 examines the second Australian case study from the same standpoint. This indicates too that the quality of the second case study findings is high. Furthermore, Section 4.3.3 uses additional information to support and/or to corroborate the opinions provided by two case study participants. In summary, Section 4.3 not only introduces the two Australian case studies, but also confirms the relationship between these two case studies and their relevance to the research questions.

4.4 Triangulation of Findings in Australia

4.4.1 Triangulation of Research Methods

Three ways methodological triangulation are used in this thesis to examine the major research question which discusses the relationship between computer forensics and different cultures. The use of three ways methodological triangulation is able to enhance the trustworthiness of the major research question. The concept of triangulation is discussed in the Section 3.4.5. In this research, the three ways that methodological triangulation are provided include historical data, Delphi survey, and case study interview. Figure 10 shows the relationship among the three different research methods.

The explanations of these three different research methods are introduced in the following three paragraphs. In addition, according to Section 4.3.3, the two case study interviews actually provide very similar results. This means that these two case studies can be considered a whole, and can be discussed together for the further triangulation issues.

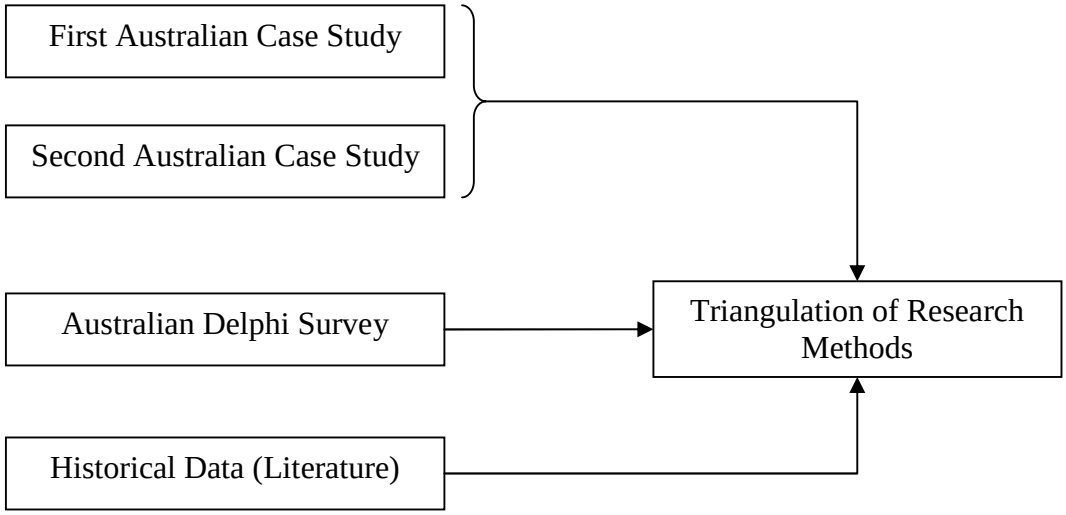


Figure 10: The Triangulation of Research Methods in Australia

First of all, the historical data, literature, proves two important concepts for this research. The first concept is that computer forensics is a subject within the field of science (Section 2.2.5), and the second concept is that some applications of science, such as science education, are affected by different cultures (Section 2.3.3). By combining these two concepts, a reasonable inference shows that computer forensic applications are affected by different cultures in certain ways.

Secondly, the interpretations of the Australian Delphi results proposed in Section 4.2.3 confirm the relationship between particular Australian behaviours within the field of computer forensics and Australian culture. Although the core concepts of 10 out of 40 questions are beyond cultural influence, the other 30 questions are explainable from a cultural perspective. In short, the discoveries of the Delphi survey are able to prove that computer forensic applications are actually affected by Australian culture.

Lastly, the interpretations of two Australian case studies, which are proposed in Section 4.3.1.2 and 4.3.2.2, demonstrate the existence of the relationship between computer

forensics and Australian culture. Question 3 is the only question which cannot be explained by a cultural perspective. The findings of Question 3 show that some values in the field of computer forensics are beyond a cultural influence. In summary, the discoveries of the case study are able to provide evidence that that certain computer forensic applications are affected by Australian culture.

In conclusion, the results of these three methods are able to corroborate the relationship between Australian culture and computer forensics. This means that methodological triangulation is achieved, and the validity of these results is improved and more convincing.

4.4.2 Corroboration for Delphi Survey and Case Study

After conducting the Australian Delphi survey and case study interviews, an interesting phenomenon is revealed. The findings of some Delphi questions essentially match the results of certain case study questions. In this case, the trustworthiness of these Delphi results is enhanced by the findings of case study interviews, and vice versa. In here, two Australian case studies are considered as a whole, since they have close answers and findings. Thus, in this section, the term '*case study*' actually represents the first Australian case study and the second Australian case study.

This section lists the corroborations for the interpretations of Delphi results and case study findings for the further verification of the relationship between computer forensics and Australian culture. The relationships between Delphi questions and case study questions can be found in the Table 13.

Table 13: Relationships between Case Study Questions and Delphi questions

Case Study Question 1	Delphi Question 5
Case Study Question 3	Delphi Question 30
Case Study Question 4	Delphi Question 17
Case Study Question 5	Delphi Question 38
Case Study Question 6	Delphi Question 14
Case Study Question 7 and 8	Delphi Question 17 and 22
Case Study Question 11	Delphi Question 36
Case Study Question 12	Delphi Question 39 and 40
Case Study Question 13	Delphi Question 22

The Delphi questions mentioned in the Table 13 are listed as follows.

- ***Question 5: From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?***
    - ***Derivative Question (Question 2 in the Round Two Delphi Questionnaire): Due to different organizations and/or different understandings, there is more than one guideline for computer forensics. Unfortunately, there is no specific SOPS for computer forensic purpose at this moment. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 14: In your country, do law enforcement organizations out-source computer forensic problems?***
- ***Question 17: How are computer forensic experts produced in your country? through what kind of tests? or procedures?***
- ***Question 22: In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?***
- ***Question 30: Based on your knowledge, have performing computer forensic investigations in your country suffered any difficulty? Can you briefly list them?***
- ***Question 36: Do you know of any difficulties caused by using digital evidence in court? If "SO", what has been the major reason for this?***

- ***Question 38: Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If "SO", does this affect the attitude of computer forensic investigators to perform investigations? If "YES", can you briefly explain?***
- ***Question 39: As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?***
- ***Question 40: As a computer forensic professional, do you use any type of encryption tools for the data in your work?***

In addition, the case study questions mentioned in the Table 13 are listed as follows.

- ***Question 1: In your organization, do you have Standard Operating Procedures (SOPS) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.***
- ***Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?***
- ***Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?***
- ***Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.***
- ***Question 6: In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.***
- ***Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?***
- ***Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?***

- ***Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?***

  B) In your own experience, what is the level of legal knowledge that members of the court have?
- ***Question 12: As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?***
- ***Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?***

The following paragraphs discuss the relationships between the Delphi questions and the case study questions. The findings of case study Question 1 not only match, but also enhance the results of Question 5 of the Round One Delphi Questionnaire. Both of the two questions confirm that various SOPs exist in different organizations in Australia. This indicates the importance of the issue of computer forensic SOPs is confirmed by two different research methods.

In Question 3 of the case study questionnaire, the two case study respondents stated that the staffing levels are not sufficient for current digital incidents. They are both planning to recruit more computer forensic investigators in the near future. These findings corroborate the outcomes of Delphi Question 30. The outcomes of Delphi Question 30 stated that the number of computer forensic investigators in Australia is not enough. In short, combining the findings of previous two questions shows that these two questions can actually enhance the trustworthiness of each other.

In Question 4 of the case study questionnaire, the findings indicates that two case study respondents are more willing to recruit a computer forensic investigator with actual experiences and great technical ability. These findings match the outcomes of Delphi Question 17, which describe the expertise and experience are two important factors in Australian culture. In conclusion, the findings of the case study Question 4 can enhance the trustworthiness of the results of the Delphi Question 17, and vice versa.

Combining the discoveries of the case study Question 5 and the results of the Delphi Question 38 shows that the imperfection of legislation does not affect the attitudes of

computer forensics investigators. In case study Question 5, ACSE 1 chooses to actively ask the Australian government to enhance legislation of related laws, and ACSE 2 considers that the government policies and his work are two different issues. In Delphi Question 38, four Delphi experts further stated that the attitudes of computer forensic investigators are not affected by incompletion of legislation. In short, case study Question 5 has similar findings to Delphi Question 38. The corroboration between these two questions is achieved.

In Question 6 of the case study questionnaire, it is discovered that law enforcement agencies (e.g. AFP and state police) and certain private accounting companies are eligible to deal with computer forensic issues. Two experts further confirmed that criminal cases are always dealt by law enforcement agencies. The findings are corroborated by the discoveries of Delphi Question 14, which agreed that law enforcement organizations do not out-source computer forensic problems. In this case, the trustworthiness of discoveries of case study Question 6 is enhanced by the findings of Delphi Question 14, and vice versa.

The finding of case study questions (Question 7 and 8) point out that on-the-job training is the major training method for computer forensic investigators in Australia. However, these findings also confirmed that there is no standard training program for computer forensic investigators. In addition, Delphi questions (Question 17 and 22) provide similar outcomes, which agreed that there are multiple ways to train a computer forensic investigator. In summary, these four questions confirm that the there are multiple training methods for computer forensic investigators in Australia at this moment.

The findings of Question 11 of the case study questionnaire corroborate the results of the Delphi Question 36. In case study Question 11, two experts stated that the members of the court should spend more time on comprehending computer forensic issues, but they do not need in-depth understanding of these issues. In addition, Question 36 of the Round One Delphi Questionnaire shows the major barrier for presenting digital evidence in the court is the understanding issue. Normally, the members of the court do not realize the characteristics of digital evidence. In short, the trustworthiness of discoveries of case study Question 11 is enhanced by the findings of Delphi Question 36, and vice verse.

The findings of case study Question 12 match the results of Delphi Question 39 and 40. Two Australian case study participants stated that they sometimes do not use data encryption and data wiping tools. These findings match the Delphi consensuses of Question 39 and 40. This indicates that the answers provided by ACSE 1 and ACSE 2 corroborate the Delphi consensuses, and vice versa. This infers that the outcomes of these three questions are proved to be more reliable.

The findings of case study Question 13 match the results of Delphi Question 22. Combining the findings of these two questions confirms that there are several methods in Australia to train a computer forensic investigator or to upgrade the skills of a computer forensic investigator. In short, the corroboration for case study Question 13 and Delphi Question 22 proves the trustworthiness of these findings.

4.4.3 Summary of Section 4.4

Section 4.4.1 shows that the concept of triangulation is achieved after examining the inference of historical data, cultural interpretations of Australian Delphi results, and cultural interpretations of Australian case study findings. The triangulation not only indicates that computer forensic applications are affected by Australian culture, but also provides a response to the research question of this thesis. In addition, triangulation further enhances the trustworthiness of the results of these three research methods. Section 4.4.2 further points out that the results of some Delphi questions are able to corroborate the outcomes of certain case study questions. The corroborations prove the trustworthiness of these questions.

4.5 Summary of this Chapter

This chapter not only lists the findings of the Australian Delphi survey and the case study interviews, but also provides cultural interpretations for these results. In the Delphi survey, although the outcomes of 10 questions (Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31) are beyond the influence of culture, the findings of the other 30 questions provide concrete proof for the relationship between computer forensics and Australian culture. In addition, Question 3 of the case study questionnaire encounters the same situation. The core concept of this question is independent, and is not affected

by different cultures. On the other hand, the other 12 case study questions can be explained by cultural accounts.

In summary, the findings of Delphi survey and case study interviews indicate that particular Australian behaviours within the field of computer forensics are explainable from cultural perspectives. The current situations of computer forensics within Australia are mainly caused by the following characteristics of Australian culture.

- Australian culture is tolerant of different opinions.
- Australian culture is willing to take on the challenge of, and face the possible uncertainty of, the future.
- Australian culture emphasizes on the expertise.
- Australian culture emphasizes on the experience.
- Australian culture puts emphasis on the initiative and achievement of an individual.
- Australian culture respects the value of independence.
- Australian culture respects the value of autonomy.
- Australian culture views the hierarchy as the arrangement for convenience.
- Australian culture believes everyone has equal right, and the supervisor is accessible.
- Australian culture shares very similar cultural background with the United States of America and Great Britain.
- Australian culture believes the value of science.
- Australian culture is easy, relaxed, and comfortable.

5 Research Findings in Taiwan

5.1 Overview of this Chapter

This chapter discusses the outcomes discovered in the Taiwanese Delphi survey and two Taiwanese case study interviews. Cultural interpretations for these findings are provided and discussed in this chapter as well. The results of the Taiwanese Delphi survey and two Taiwanese case study interviews are listed in Section 5.2.2, Section 5.3.1.1, and Section 5.3.2.1 correspondingly. These results are discussed, as in the previous chapter by dimensions.

In addition, interpretations of the Taiwanese Delphi results are provided in Section 5.2.3, and these have been made to elucidate the Taiwanese Delphi results from a cultural perspective. Similar cultural interpretations of two Taiwanese case studies outcomes can be found in Section 5.3.1.2 and 5.3.2.2. Lastly, Section 5.4 combines the cultural interpretations of the Delphi outcomes with the cultural interpretations of case studies results, and provides overall conclusions for the modern conditions of computer forensics in Taiwan. These conclusions will be further used to compare with the Australian conclusions in Chapter 6 so as to produce cross-nations discussions.

5.2 Delphi Survey

A Delphi survey cannot be performed without enough respondents. However, the number of computer forensic workers in Taiwan is limited. These two conflicting conditions created a tough challenge for the researcher. The researcher successfully invited 10 computer forensic experts to participant in this Delphi survey. The details of the number of respondents are discussed in Section 3.5.7 (Delbecq et al 1986; Dalkey 1969; Clayton 1997; Fitch *et al* 2001). These 10 respondents were coming from different backgrounds. Five of them come from academia, one of them has a legal background, and four of them are practical computer forensic investigators. This means that the trustworthiness of their opinions is qualified. The discussions of these experts can be found in Section 5.2.1.

Instead of listing the Delphi results by rounds, this thesis lists the results of Taiwanese Delphi survey by dimensions in Section 5.2.2, and also shows the cultural interpretations of these Delphi results by dimensions in Section 5.2.3. This is because the purpose of the Taiwanese Delphi survey is to show the characteristics of Taiwanese cultural perspectives rather than the process of consensus of each question.

5.2.1 Experts of the Delphi Survey

The Taiwanese respondents for the Delphi survey must be chosen deliberately to reflect the latest conditions of computer forensics because computer forensics is a specialist subject which needs manpower with exclusive knowledge. In Taiwan, computer forensic experts mainly exist in two areas, law enforcement, and academia. Investigators with computer forensic background normally belong to government bureaus or agencies, such as Ministry of Justice, Investigation Bureau (MJIB), and Criminal Investigation Bureau (CIB). In addition, there are several universities officially teach computer forensic courses. Most of the academic researchers, who participate in the Delphi survey, are involved in the computer forensic field by personal interest, or by the academic cooperation with Professor I-Long Lin of the Central Police University.

The researcher successfully invited ten Taiwanese respondents with different backgrounds to participate in the Delphi survey. These ten computer forensic experts consisted of five academic researchers, one legal expert, and four computer forensic practitioners. The number, *ten*, not only meets the requirements of a Delphi survey, but also is large enough to represent the current conditions of computer forensics in Taiwan.

5.2.2 Findings of Delphi Survey

There are 40 different questions in the Delphi questionnaire (Chinese version) given in the Appendix 5, and these are classified into 11 sub-sections. These 11 sub-sections are further categorized into 5 dimensions, which are *Current Situation, Policy and Organization, Education, Law*, and *Personal Preferences and Skills*.

Ten Taiwanese computer forensic experts were invited to participant in Taiwanese Delphi survey, and every expert completed the entire Delphi process, including the Round One survey and the Round Two survey. In this thesis, 70% is used as the criterion to decide the accomplishment of the Delphi consensus. There were 11 questions did not reach the consensus in the Round One Delphi survey. Thus, the feedback from these 11 questions was managed, and was used to form the Round Two Delphi questionnaire (Chinese version), which is listed in Appendix 6. The English version of the Round Two Delphi questionnaire (Chinese version) is listed in Appendix

7. Every question in the Round Two Delphi questionnaire reached consensus, and no further (Round Three) questionnaire was needed.

In the following 5 sections (from Section 5.2.2.1 to Section 5.2.2.5), this thesis lists the Delphi findings based on the 5 dimensions rather than the sequence of the questions in the Round One Delphi questionnaire. There are two reasons for this arrangement. The first reason is that the sequence of the sub-sections is listed randomly so as to prevent participants guessing the answers which were desired by the researcher. The second reason is that this arrangement provides a better understanding of computer forensic phenomena from cultural perspectives. It is pertinent to describe the possible cultural differences between Australia and Taiwan by the 5 dimensions.

5.2.2.1 Current Situation Dimension

The Current Situation Dimension contains Section 1, 2, 3, and 8. There are 17 different questions in total. Question 3, 5, 8, 9, 10, and 28 did not reach the required consensus, and became Question 1 to 5, and 10 in the Round Two Delphi questionnaire. Table 14 not only shows the condition of consensus and agreement of each question within this dimension, but also describes the relationship between questions, which did not reach the consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 14: Condition of Consensus and Agreement of Each Question within Current Situation Dimension

	Consensus	Agreement (%)
Round 1, Question 1	Y	90%
Round 1, Question 2	Y	80%
Round 1, Question 3	**N**	**N/A**
=>Round 2, Question 1	**Y**	**80%**
Round 1, Question 4	Y	70%
Round 1, Question 5	**N**	**50%**
=>Round 2, Question 2	**Y**	**90%**
Round 1, Question 6	Y	100%
Round 1, Question 7	Y	70%
Round 1, Question 8	**N**	**N/A**
=>Round 2, Question 3	**Y**	**70%**
Round 1, Question 9	**N**	**N/A**
=>Round 2, Question 4	**Y**	**90%**
Round 1, Question 10	**N**	**N/A**
=>Round 2, Question 5	**Y**	**70%**
Round 1, Question 11	Y	70%
Round 1, Question 12	Y	70%
Round 1, Question 27	Y	90%
Round 1, Question 28	**N**	**N/A**
=>Round 2, Question 10	**Y**	**80%**
Round 1, Question 29	Y	70%
Round 1, Question 30	Y	100%
Round 1, Question 31	Y	70%

5.2.2.2 Policy and Organization Dimension

The Policy and Organization Dimension contains Section 4 and 9. There are 7 different questions in total. Question 15 did not reach the requirement of consensus, and became Questions 6 in the Round Two Delphi questionnaire. Table 15 not only shows the condition of consensus and agreement of each question within this dimension, but

also describes the relationship between Question 15 in the Round One Delphi questionnaire and Question 6 in the Round Two Delphi questionnaire.

Table 15: Condition of Consensus and Agreement of Each Question within Policy and Organization Dimension

	Consensus	Agreement (%)
Round 1, Question 13	Y	70%
Round 1, Question 14	Y	90%
Round 1, Question 15	**N**	**60%**
=>Round 2, Question 6	**Y**	**90%**
Round 1, Question 16	Y	80%
Round 1, Question 32	Y	90%
Round 1, Question 33	Y	90%
Round 1, Question 34	Y	100%

5.2.2.3 Education Dimension

The Education Dimension contains Section 5 and 6. There are 7 different questions in this dimension. Question 21 and 23 did not reach the requirement of consensus, and became the Question 7 and 8 in the Round Two Delphi questionnaire. Table 16 not only shows the condition of consensus and agreement of each question within this dimension, but also describes the relationship between questions, which did not reach the consensus, in the Round One Delphi questionnaire and subsequent questions in the Round Two Delphi questionnaire.

Table 16: Condition of Consensus and Agreement of Each Question within Education Dimension

	Consensus	Agreement (%)
Round 1, Question 17	Y	80%
Round 1, Question 18	Y	70%
Round 1, Question 19	Y	70%
Round 1, Question 20	Y	90%
Round 1, Question 21	**N**	**60%**
=>Round 2, Question 7	**Y**	**90%**
Round 1, Question 22	Y	70%
Round 1, Question 23	**N**	**N/A**
=>Round 2, Question 8	**Y**	**80%**

5.2.2.4 Law Dimension

The Law Dimension contains Section 10, and there are 4 different questions in this dimension. Question 35 did not reach the requirement of consensus, and became Questions 11 in the Round Two Delphi questionnaire. Table 17 not only shows the condition of consensus and agreement of each question within this dimension, but also describes the relationship between Question 35 in the Round One Delphi questionnaire and Question 11 in the Round Two Delphi questionnaire.

Table 17: Condition of Consensus and Agreement of Each Question within Law Dimension

	Consensus	Agreement (%)
Round 1, Question 35	**N**	**60%**
=>Round 2, Question 11	**Y**	**90%**
Round 1, Question 36	Y	90%
Round 1, Question 37	Y	70%
Round 1, Question 38	Y	80%

5.2.2.5 Personal Preferences and Skills Dimension

The Personal Preferences and Skills Dimension contains Section 7 and 11. There are 5 different questions in total. Question 25 is the only question did not reach the requirement of consensus, and became Questions 9 in the Round Two Delphi questionnaire. Table 18 not only shows the condition of consensus and agreement of each question within this dimension, but also describes the relationship between Question 25 in the Round One Delphi questionnaire and Question 9 in the Round Two Delphi questionnaire.

Table 18: Condition of Consensus and Agreement of Each Question within Personal Preferences and Skills Dimension

	Consensus	Agreement (%)
Round 1, Question 24	Y	90%
Round 1, Question 25	**N**	**60%**
=>Round 2, Question 9	**Y**	**80%**
Round 1, Question 26	Y	70%
Round 1, Question 39	Y	70%
Round 1, Question 40	Y	90%

5.2.3 Interpretations of Delphi Results

Ten Delphi respondents provided their professional opinions based on their practical experiences. Ten Delphi respondents consisted of one legal expert, four academic researchers, and five computer forensic practitioners. The cultural interpretations are given for these Delphi findings. In addition, further interpretations are given for certain questions. This is because the findings of some questions may be supported by the outcomes of other questions. In this case, the trustworthiness of these interpretations is improved by the cross-question corroborations.

There are three standpoints should be clearly explained. The first standpoint is that the questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire are discussed together. For example, Question 7 in the Round One Delphi questionnaire and Question 2 in the Round Two Delphi questionnaire are considered a single concept, and are treated together. This is

reasonable since Question 2 in the Round Two Delphi questionnaire is actually seeking consensus for the Question 7 in the Round One Delphi questionnaire.

The second point of note is that not every single question has a reasonable cultural explanation. For example, Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31 are caused by global and independent values rather than cultural reasons. Thus, they do not have cultural explanations.

Lastly, the third reason is that Question 11 and 23 can only be perfectly explained unless they are merged with Australian feedback. Combining the Australian and Taiwanese findings of Question 11 (or Question 23) is able to distinguish the different attitudes in Australian and Taiwanese cultures. In short, there are three different types of explanations. The first type of explanation is that there are reasonable cultural explanations for most questions. The second type of explanation is that 10 questions (Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31) whose global and independent values are not affected by different cultures. Lastly, the third type of explanation is that some questions, such as Question 11 and 23, are only meaningful with Australian feedbacks.

5.2.3.1 Current Situation Dimension

There are 17 questions in total in this dimension, and they are: Question 1 to 12, and 27 to 31. Most of these questions reached the consensus except Question 3, 5, 8, 9, 10, and 28. These six questions became Question 1 to 5, and 10 in the Round Two Delphi questionnaire respectively. Fortunately, these six questions in the Round Two Delphi questionnaire reached the 80%, 90%, 70%, 90%, 70%, and 80% agreement correspondingly. In summary, 17 questions in this dimension reached the consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed below.

- ***Question 1: From your point of view, what is your government's perspective on computer forensic issues? Do you think the emphasis they put on it is currently at an appropriate level?***
- ***Question 2: What is your opinion on the current developments within computer forensics? Are you satisfied with the current developments of***

computer forensics? Why?

- ***Question 3: How many years has computer forensics existed as a discipline in your country?***
    - ***Derivative Question (Question 1 in the Round Two Delphi Questionnaire): In Taiwan, computer forensics was developed around 5 years ago, and the Cyber Forensics Laboratory was established at the end of 2006. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 4: Is computer forensics a topical issue in your country?***
- ***Question 5: From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?***
    - ***Derivative Question (Question 2 in the Round Two Delphi Questionnaire): Due to different organizations and/or different understandings, there is more than one guideline for computer forensics (confirmed by 2.1). Unfortunately, there is no specific SOPS for computer forensic purpose at this moment. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***

Question 6: What is your opinion on the importance of SOPs of computer forensic investigations?

- ***Question 7: Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?***
- ***Question 8: Based on your knowledge, what are the main characteristics of digital evidence? (e.g. Integrity)***
    - ***Derivative Question (Question 3 in the Round Two Delphi Questionnaire): According to the table, the characteristics can be classified into 12 different categories. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 9: What is your opinion on meta-data of digital evidence from computer forensic perspective?***

(Derivative Question (Question 4 in the Round Two Delphi Questionnaire): The meta-data (e.g. time stamp) of digital evidence plays an important role in a computer forensic investigation. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)

- ***Question 10: What is your opinion on the trustworthiness of meta-data of digital evidence?***
    - ***Derivative Question (Question 5 in the Round Two Delphi Questionnaire): As long as the procedures and computer forensic tools are correct, the reliability of meta-data of digital evidence is not a problem. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 11: How would you describe the relationship between computer security and computer forensics?***
- ***Question 12: When performing a computer forensic investigation, is it necessary to understand the background of the investigated person? (How many dogs they have? What cars they drive? Do they have any habit?) or just focus on analysing the digital data? Why?***
- ***Question 27: Based on your knowledge, have computer forensic investigations in your country ever encountered problems which are caused by time-stamps? or by different time zones? If "YES" how you deal this type of problems?***
- ***Question 28: Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%***
    - ***Derivative Question (Question 10 in the Round Two Delphi Questionnaire): In Taiwan, a computer forensic investigation reasonable encounters 0%-20% encrypted data. In the worst situation, a computer forensic investigation encounters at most 40% encrypted data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 29: Based on your knowledge, how do computer forensic investigators deal with the encrypted data in your country?***
- ***Question 30: Based on your knowledge, have performing computer forensic investigations in your country suffered any difficulty? Can you briefly list them?***
- ***Question 31: "Technical Issues" and "Human Issues" are two separate things. It is easy to examine misuse of a computer, but how to prove the suspect is the one who actually caused this misuse is not an easy task. Based***

on your knowledge, how do computer forensic investigators deal with this problem in your country?

In Question 1, nine Delphi experts agreed that Taiwanese government does realize the importance of computer forensics. The only exception is that one computer forensic practitioner stated that Taiwanese government does not put emphasis on computer forensics.

Eight experts stated that the development of computer forensics can be improved in Question 2. Two Delphi respondents, who work as computer forensic practitioners, have different opinions. One of them stated that the development of computer forensics is acceptable, and the other expert did not provide his opinion.

The findings in Question 3 can be mainly classified into five categories. There is no explicit agreement for this question. Delphi respondents provided various opinions for this question. Thus, Question 1 of the Round Two Delphi questionnaire is created to seek for the Delphi consensus. Fortunately, 80% agreement was achieved, and the consensus shows eight experts agreed that computer forensics has existed as a discipline for 4 to 5years ago.

Cultural explanations can be provided for the findings of Question1, 2, and 3. In here, three questions are discussed as a whole. Taiwanese culture is deeply affected by Confucianism (Jingpan 1990; Ho 1991). However, Confucianism does not focus on the value of science. In this research, the meaning of science means Western scientific values. Thus, the value of science is not main stream in Taiwanese culture. This situation leads to a reasonable conclusion which explains that Taiwanese culture is used to following the lead of Western science within the field of science. Therefore, it is understandable that Taiwanese government started to put an emphasis on computer forensics around 4 to 5 years ago since computer forensics has obtained attention in the Western science for at least 9 years, which is proved indirectly by the paper (Scientific Working Group on Digital Evidence 1999). This paper shows that the FBI already published standards and principles for digital evidence on 1999 (9 years ago). This infers that FBI must have started relevant research before 1999. This situation can also provide a logical account for Question 2. It is reasonable for ten Delphi respondents to state that the development of computer forensics needs to be improved because the

development of computer forensics is continuous even in the United States of America or Great Britain, who are two leading Western countries having research results in computer forensics. If they are still improving the developments of computer forensics, it makes sense that Delphi consensus shows that the improvements of computer forensic development is necessary in Taiwan.

In Question 4, seven Delphi respondents, including four academic researchers and three computer forensic practitioners, stated that computer forensics is not a topical subject in Taiwan. In general, computer forensics is only a topical subject in academia and law enforcement. This situation is understandable, and is very common in the rest of the world. Due to the uniqueness of computer forensics, it is meant to be a special subject for a small group of people, such as academic researchers and computer forensic investigators. In addition, traditional forensic science (e.g. DNA and fingerprint) encounters similar situations. In short, the forensic science, including computer forensics, is a subject or topic for experts rather than for the general population. It is understandable that the Delphi respondents agreed that computer forensics is not a topical issue in Taiwan.

In Question 5, five experts, including two academic researchers and three computer forensic practitioners, described that there are computer forensic guidelines at present, such as Section 14 of Chapter 6, Investigating Principles for Police Force (Ministry of the Interior 2003). However, the computer forensic guidelines proposed by them are very general yet specific. Conversely, three Delphi respondents stated that there are no computer forensic SOPs at this moment. In addition, the other two Delphi respondents claimed that they are not familiar with this issue. Fortunately, 90% agreement was achieved for the Question 2 of the Round Two Delphi survey. These nine Delphi respondents agreed that specific SOPs do not exist at present.

With no disagreement, every expert stated that SOPs are a very important issue within the field of computer forensics. This means 100% agreement was achieved for Question 6, and also infers that the understanding of the importance of SOPs is cross-disciplinary. Delphi experts with different backgrounds all agreed on the importance of computer forensic SOPs.

In Question 7, seven Delphi experts, consisting of two academic researcher, one expert with a legal background, and four computer forensic practitioners, stated that there is no regulation for a time period to keep digital evidence after the trial. A further analysis shows that computer forensic practitioners have more understanding about this issue.

Question 5, 6, and 7 can be explained together by the typical Taiwanese cultural attitude. First of all, the findings of Question 6 need to be interpreted. In Question 6, every Delphi respondent believed in the importance of computer forensic SOPs. In addition, they further mentioned that having computer forensic SOPs is helpful when presenting digital evidence in a court of law. This infers that they not only realize that SOPs are very important for technical purposes, but also are significant for the legal purposes. In summary, this is the fundamental consensus for every computer forensic worker despite their nationalities and professional backgrounds. Moreover, this concept leads to a cultural interpretation for Question 5. The importance of computer forensic SOPs is confirmed. However, according to Delphi consensus (Question 5), only general computer forensic guidelines exist at this moment, and there are currently no computer forensic SOPs. In addition, two Delphi experts who work for the law enforcement agency admitted that computer forensic SOPs do not exist at present. This shows that Taiwanese culture tends to avoid possible uncertainties. Changing may encounter unpredicted consequences. Thus, Taiwanese normally focus more on short-term rather than long-term objectives. In this case, the core of the problem is sometimes ignored. This explains why there are no computer forensic SOPs although every computer forensic worker realize its importance. In addition, this cultural attitude can also explain the Delphi consensus of Question 7. Delphi experts stated that there is no regulation which defines the time period to keep digital evidence after the trial. According to Delphi consensus (Question 3), computer forensics has been developed for around 4 to 5 years in Taiwan. This infers that the proper legislation can be made to define the time issues of digital evidence preservation in this period. However, this type of regulation does not exist at this moment. This echoes the previous proposed standpoint. In summary, the standpoint for Question 5 and 7 are reasonable and trustworthy since Hofstede (1980) proposed the similar interpretation to describe the nature of Taiwanese culture. He believed that Taiwanese culture has strong uncertainty avoidance. This indicates that changing the current situation is always the last choice in Taiwanese culture.

There is no clear agreement for the Question 8 of the Round One Delphi questionnaire. Delphi experts viewed the characteristics of digital evidence from different perspectives and proposed many different opinions. Fortunately, Question 3 of the Round Two Delphi survey reached the 70% agreement. In summary, Delphi respondents stated the characteristics of digital evidence mainly are: integrity, hard to identify original users, original data is not understandable, and easy to damage. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. There are two reasons for this situation. The first reason is that the findings of this question are the basic and essential understanding of digital evidence. Like addition in the field of mathematics, culture cannot affect the result of one plus one. In addition, the second reason is that computer forensic experts must have basic computer knowledge, and usually have adequate understanding of computer security issues. The way they learn the essential knowledge of computer is very similar. Thus, it is not surprising that they proposed similar characteristic for digital evidence despite their nationalities and cultural backgrounds.

The findings in Question 9 can be mainly classified into five categories. There is no explicit agreement for this question. Various opinions were provided for this question. Thus, Question 4 of the Round Two Delphi survey was created to seek for the Delphi consensus. Fortunately, 90% agreement was achieved for Question 4 of the Round Two Delphi questionnaire. This means that nine Delphi respondents agreed that the meta-data (e.g. time stamp) of digital evidence plays an important role in a computer forensic investigation. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. The importance of meta-data of digital evidence is a fundamental understanding within the field of computer forensics, and this is not affected by the different cultures.

The findings in Question 10 can be mainly classified into five categories. There is no explicit agreement for this question. Most Delphi experts believed that the trustworthiness of meta-data of digital evidence is not a serious problem. Nevertheless, some of them did not completely agree with its trustworthiness. 70% agreement was achieved for Question 5 of the Round Two Delphi questionnaire. In conclusion, Delphi respondents believed that the trustworthiness of meta-data of digital evidence is based on the reliability and validity of computer forensic tools and proper computer forensic procedures. If the computer forensic tool is sound and/or the computer forensic

procedures are correct, meta-data of digital evidence is firm and solid as well. This demonstrates that Taiwanese culture puts more focus on the unambiguous truth. People in Taiwan are used to seek for the only answer of a problem. They have sought for the correct answer since elementary school. People in Taiwan are always taught that there is only one correct answer for a question. Thus, it is understandable that Taiwanese culture would like to ensure the trustworthiness of meta-data of digital evidence as clear as possible., Hofstede (1980) stated that one of the typical attitudes of strong uncertainty avoidance is "*The search is for ultimate, absolute truths and values.*". The cultural interpretation of this question is corroborated by Hofstede's statement.

70% agreement was achieved for Question 11. In Taiwan, the Delphi experts considered computer security and computer forensics are two separated topics, but they also thought that computer security and computer forensics work and cooperate as a cycle. Computer security is the front end of this cycle, and computer forensics is the back end of this cycle. Better computer security is helpful for computer forensics. This is because better computer security may be able to save more traces for computer forensic purposes. In addition, the capability of computer forensics can enhance the quality of computer security. It is believed that computer forensics has the ability to point out the weaknesses of computer security. Since these two subjects are essentially similar to each other, it is not surprising that Taiwanese culture treat them as part of a cycle. In addition, Hofstede (1980) also proved this argument by describing Taiwanese culture is more feminine than masculine. This means that Taiwanese culture tends to consider things more interdependently than independently. In short, the cultural interpretation of this question is enhanced by Hofstede's findings.

70% agreement was achieved for the Question 12. This means that seven Delphi respondents, including four academic researchers and three computer forensic practitioners, agreed that understanding the background of the suspect is helpful for a computer forensic investigation. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. In reality, multiple data sources are usually used to prove the guilt or the innocence of the suspect. Various types of evidence (e.g. physical evidence and digital evidence) and/or any useful information are usually required for a legal case. Thus, the Delphi consensus of this question is understandable.

In Question 27, besides the only expert with a legal background, the other nine Delphi respondents agreed that the time issues, which are caused by time-stamps and/or different time zones, are not a serious problem for a computer forensic investigation. This situation is believed to be for two reasons. The first reason is that there is only one time zone within Taiwan. Thus, computer forensic investigators would not expect to encounter different time issues of digital evidence. In addition, the second reason is that time related issues are the first concern when computer forensic investigators analyse digital evidence. Despite the different backgrounds of these nine Delphi experts, most of them stated that time issues are the fundamental concern and the basic understanding for computer forensic investigators. This infers computer forensic investigators in Taiwan would pay additional attention to the time-stamp of digital evidence and/or the time zone setting of the seized computer because of their training.

The findings in Question 28 can be mainly classified into five categories. There was no explicit agreement for this question. Delphi respondents provided various opinions for this question. Thus, Question 10 of the Round Two Delphi survey was created to seek the Delphi consensus. Fortunately, 80% agreement was achieved for Question 10 of the Round Two Delphi questionnaire. This means that eight Delphi respondents agreed that a computer forensic investigation reasonable encounters 0%-20% encrypted data, and at most 40% encrypted data in the worst situation. The findings of this question (Question 10 of the Round Two Delphi questionnaire) conflict to the results of Question 40. According the Delphi consensus of Question 40, it is reasonable for people in Taiwan to use encryption tools to protect their privacy and the confidentiality of the data. This is mainly because of the competitive living environment. Competition is usually necessary for best results for an individual in work, education and basic life. This explanation is supported by Hofstede (1980). Hofstede believed that Taiwanese culture has strong uncertainty avoidance, and described that "*Higher anxiety and stress are experienced.*" as one of the typical behaviours in the strong uncertainty avoidance society. In this case, it is not surprising that Taiwanese people try to use certain actions to release the stress. However, the findings of this question (Question 10 of the Round Two Delphi questionnaire) show that a computer forensic investigation normally encounters 0%-20% encrypted data. The possible explanation for this is that the technical issues within the field of computer science are not completely understood by people in Taiwan. Otherwise, the findings of this question (Question 10 of the Round Two Delphi questionnaire) should match the results of Question 40.

70% agreement was achieved for the Question 29. This means that seven Delphi respondents agreed that decryption is the major way to deal with encrypted data. In here, decryption has several meanings, such as brute force and password guessing. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. Culture cannot affect the pure technical skills and/or issues. For example, culture cannot affect the result of one plus one. In short, despite the different cultures, decryption is a reasonable method to deal with encrypted data.

Ten Delphi respondents all agreed that the computer forensic investigations encounter certain difficulties. This means that 100% agreement was achieved for Question 30. In addition, these difficulties mainly include lack of manpower, lack of equipments, lack of understanding, lack of proper training, and lack of educational courses. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. Within the field of computer forensics, similar difficulties are occurring in the rest of the world. Since the budget from the government is always limited, it is understandable that there is always not enough money to purchase the latest computer forensic equipments, to recruit more employees, and to set up educational courses. In short, these difficulties can be considered cross-national and cross-cultural issues, and are common phenomena in the field of computer forensics.

In Question 31, seven Delphi experts agreed that using other method (e.g. surveillance cameras) and/or evidence (e.g. fingerprints) is helpful to build the relationship between the suspect and the misuse of a computer. However, two out of the other three Delphi respondents, who work as computer forensic practitioner, stated that this issue does not belong to the job of a computer forensic investigator. They believed that they are only responsible for the validity of digital evidence. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. It is common to use other methods and/or data sources, such as surveillance cameras and fingerprints, to establish the relationship between the suspect and the misuse of a computer. Using other methods is a universal skill to prove the guilt or innocence of the suspect, and is not affected by different cultures.

5.2.3.2 Policy and Organization Dimension

Question 13 to 16, and 32 to 34 were designed for this dimension in the Round One Delphi questionnaire. Every question reached the consensus except Question 15, which became Question 6 in the Round Two Delphi questionnaire. Fortunately, Question 6 in the Round Two Delphi questionnaire reached 90% agreement. In summary, seven questions in this dimension reached the consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed below.

- ***Question 13: In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?***
- ***Question 14: In your country, do law enforcement organizations out-source computer forensic problems?***
- ***Question 15: Does the organization/department/agency you work for have policies for computer forensic readiness? If "YES", can you provide the name of your organization/department/agency? could you please briefly explain the policies.***
    - ***Derivative Question (Question 6 in the Round Two Delphi Questionnaire): Generally speaking, in Taiwan, practical organizations (e.g. MJIB) have facilities, processes, and ability for computer forensic issues, but non- practical organizations (e.g. university) do not have equivalent preparations and needs. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 16: In your country, are computer security issues and computer forensics issues dealt by different organization/department/agency? If "YES", how would you describe the relationship between computer security organization/department/agency and computer forensic organization/department/agency?***
- ***Question 32: Based on your knowledge, have computer forensic organizations/departments/agencies in your country ever had interactions with international organizations/departments/agencies related to similar area? If "YES", how do they interact with other organizations/departments/agencies in other countries?***

- ***Question 33: Based on your knowledge, in your country have computer forensic educational researchers ever had interactions with private/government computer forensic organizations/departments/agencies? If "YES", how do they interact with each other?***
- ***Question 34: Based on your knowledge, employees in the field of computer forensics normally interact or share their professional experiences with (1)colleague (2)supervisor (3)others (please explain)***

70% agreement was achieved in Question 13. Seven experts stated that the computer forensic organizations are central (federal-level) organizations yet local (state-level) organizations within the police system. The other three experts believed that the status of computer forensic organizations is either lower or equal to the status of general police duties, and these three experts are all computer forensic practitioners. This phenomenon can be explained by the following perspective. It is believed that the importance and the development of computer forensics are not completely realized by the Taiwanese government. This statement is proved by the Delphi consensus of Question 2 of the Round One questionnaire. After all, the central (federal-level) computer forensic organizations do not have enough resources to cope with every digital incident within Taiwan. This situation infers that Taiwanese culture tends to avoid possible uncertainties. As long as the solution exists, the quality of the solution is not going to be discussed. Thus, the essence of the issue is sometimes overlooked. Hofstede (1980) used a similar concept to describe that the uncertainty avoidance is one of the characteristics of Taiwanese culture. His argument supports the cultural interpretation of this question.

In Question 14, nine experts agreed with this question except one computer forensic expert. The only computer forensic expert, having the different opinion, did not answer this question due to lack of reliable data resources. The findings of this question are very likely to be caused by two reasons, which consist of one cultural explanation and one acultural explanation. The cultural reason is explained by the different values and beliefs between in-group and out-group. In Taiwan, a neutral organization can rarely be found, since Taiwanese culture believes that the value is different between in-group and out-group. This indicates that the results, which are produced by the people in out-group, are sometimes hard to be believed by the people in in-group. This argument is supported by Hofstede (1980). He stated that Taiwanese culture is built around

collectivism rather than individualism, and "*Value standards differ from in-groups and out-groups.*" is one of typical features of collectivism. This indicates that the cultural explanation of this question is trustworthy. In addition, the acultural reason is satisfied by the nature of digital evidence. Due to the uniqueness of digital evidence, it is understandable that law enforcement agencies do not out-source digital evidence investigation. The validity and reliability of digital evidence are of most concern when presented in a court of law.

The finding in Question 15 shows that six experts agreed that there is no computer forensic readiness in their organizations. This indicates that the agreement of Question 15 was 60%, and did not reach Delphi consensus. Fortunately, three experts changed their minds in Question 6 of the Round Two Delphi survey. Nine experts agreed that the computer forensic readiness is needed in practical organizations, and non-practical organizations do not have urgent need to set up the computer forensic readiness. The only expert, who did not agree with this issue, is a computer forensic practitioner. The findings of this question can be explained by the following cultural reason. Taiwanese culture normally focuses on short-term issues, and wants to have immediate results. This means the consequences and long-term issues are sometimes overlooked. The solutions for the possible troubles in the future are not discussed and worried about until urgent need arises. Not surprisingly, the Delphi experts agreed that non-practical organizations do not have urgent needs for preparing for computer forensic readiness. This statement matches the finding of Hofstede's research (1980). He described that avoiding changes is a typical cultural attitude in Taiwanese culture.

In Question 16, eight experts, including four academic researchers and four computer forensic practitioners, stated that computer security issues and computer forensic issues are dealt by different organizations. Two of them further stated that these two types of organizations cooperate with each other. This phenomenon can be explained by the following cultural perspective. Since the development of science is not superior in Taiwan, Taiwanese government obtain the information of computer forensics from Western countries (e.g. the United States of America). This argument is discussed in the Delphi Question 1, 2, and 3.

In this case, the Taiwanese government realizes that computer security and computer forensics are two similar but different topics, and they are treated differently by Western countries. In short, this explanation satisfies the Delphi consensus of this question.

90% agreement was achieved in Question 32. Nine Delphi respondents agreed that there are interactions between local computer forensic organizations and foreign computer forensic organizations. The other one expert claimed that he is not familiar with this issue. The interactions with international computer forensic organizations can be explained by the following cultural reason. People in Taiwan realize that the Western countries are usually in the leading position within the field of science. This is reasonable since Confucianism has been well-accepted in Chinese culture, which is the origin of Taiwanese culture, for thousand years. Unfortunately, Confucianism does not place enough attention on science (Jingpan 1990; Ho 1991; Slay 2000b). In here, the term 'science' represents Western scientific values. Thus, interacting with international computer forensic organizations offers a good opportunity to improve the current status and development of computer forensics in Taiwan.

90% agreement was achieved in Question 33. Nine Delphi respondents agreed that there are interactions between local computer forensic organizations/workers and local computer forensic organizations/workers. In here, computer forensic workers include academic researchers and computer forensic practitioners. One expert claimed that he is not familiar with this issue. The reason for this is that people in Taiwan rely deeply on interpersonal relationship. The importance of interpersonal relationship within Taiwanese culture is also observed by Hofstede (1980). He stated that interdependence and people are important in Taiwanese culture since Taiwanese culture is more feminine than masculine. According to the result of the Delphi survey, there are interactions between computer forensic organizations/workers and computer forensic organizations/workers, since there are not many employees devoting themselves to the field of computer forensics. A good interpersonal relationship is important in this small group. In short, this explanation satisfies the Delphi consensus of this question.

100% agreement was achieved in Question 34. Eight out of ten Delphi respondents stated that they share their professional knowledge with their colleagues. In addition, only two out of ten respondents claimed that they share their professional knowledge with their supervisors. This phenomenon can be explained by the following perspective. Taiwanese culture usually considers that the superior is inaccessible, and people in

Taiwan typically do not interact with their superior unless they have to. The nature of Taiwanese culture shows that the respects for elders and superiors are important and necessary. This indicates that there is an invisible gap between supervisors and subordinates. This cultural attitude explains the Delphi findings of this question.

In addition, this cultural explanation is provided by Hofstede (1980) and the concept of Confucianism (Jingpan 1990; Ho 1991). According to Hofstede, Taiwanese culture has large power distance. This indicates that within Taiwan hierarchy is built essentially for inequality. Moreover, there are 5 social relationships proposed by Confucianism that control the power balance with in society and always present a superior and an inferior within any relationship; *father and son*, *ruler and subject*, *husband and wife*, *elder and younger brother*, and *friend and friend* (Poh-Ling 1997). With no doubt, this shows that hierarchy and interpersonal relationship are two important features within Confucianism. In short, the cultural explanation of this question is reasonable.

5.2.3.3 Education Dimension

Seven questions, Question 17 to 23, were designed for this dimension in the Round One Delphi questionnaire. Only Question 21 and 23 did not reach the consensus, and became Question 7 and 8 in the Round Two Delphi questionnaire. Fortunately, Question 7 and 8 in the Round Two Delphi questionnaire reached 90% and 80% agreement respectively. In summary, seven questions in this dimension reached the consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed as follows.

- ***Question 17: How are computer forensic experts produced in your country? through what kind of tests? or procedures?***
- ***Question 18: Do you allow computer forensic experts from other countries to work in a similar job in your country?***
- ***Question 19: Does your country have any organization/department/agency for certifying computer forensic experts? If "YES", what are the names of the organizations/departments/agencies? What criteria do they follow?***
- ***Question 20: Is there any government organization/department/agency willing to support the education/training of computer forensic manpower? or***

to support the research of computer forensics? Can you briefly explain how the government organization/department/agency supports these agencies?

- ***Question 21: Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this program come from?***
    - ***Derivative Question (Question 7 in the Round Two Delphi Questionnaire): In Taiwan, there indeed are on-the-job training for computer forensic investigators, and these training are mainly held without a fixed schedule. The teachers come from different sources although they are all computer forensic experts. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 22: In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?***
- ***Question 23: Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?***
    - ***Derivative Question (Question 8 in the Round Two Delphi Questionnaire): Training an investigator to become a computer forensic investigator at least needs one year. After that, a computer forensic investigator needs to update and to learn all the time. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***

In Question 17, eight experts agreed that there are certain methods to form computer forensic experts in Taiwan. In addition, their answers also infer that there is no standard method for producing computer forensic experts in Taiwan. There are many works to do for improving the current situation.

70% agreement was achieved in Question 18. However, three out of seven experts stated that there is no real example at this moment. In addition, the other three computer forensic practitioners did not agree with this question. The findings of this question are explainable from the cultural perspective. Due to the influence of Confucianism, science, which represents Western scientific values, is not an important subject in Taiwan (Jingpan 1990; Ho 1991; Slay 2000b). Thus, it is reasonable that there is no outstanding

research result for the scientific issues in Taiwan. Since people in Taiwan realize this situation, inviting foreign experts becomes an alternative method. A cultural explanation corresponds to the findings of this question.

In Question 19, seven experts agreed that there is no organization for certifying the qualification of a computer forensic expert. The seven experts consisted of three academic researchers and four computer forensic practitioners.

90% agreement was achieved in Question 20. Nine experts stated that the Taiwanese government is willing to support the education and training within the field of computer forensics. For example, holding conferences and sending computer forensic investigators to vendor-based courses are two popular ways. The findings of this question can be explained by the following cultural reason. The importance of science (Western scientific values) is sometimes not of concern in Taiwanese culture because of the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). In the field of science, Taiwanese usually follow the lead of Western countries (e.g. the United States of America and Great Britain). This standpoint is explained in Delphi Question 1, 2, and 3. This indicates that Taiwanese government realizes that the development of computer forensics in Taiwan is not perfect, and there is much work needing to be done so as to keep up with the leading countries. Therefore, it is understandable for Taiwanese government to show supportive attitudes for the computer forensic education, training, and research.

The finding in Question 21 shows that six experts, including three academic researchers and three computer forensic practitioners, agreed that there is on-the-job training for computer forensic investigators. However, 60% agreement was not enough for Delphi consensus. Fortunately, three experts changed their minds in Question 7 of the Round Two Delphi survey. This means that 90% agreement was reached for Question 7 of the Round Two Delphi questionnaire. Besides the cultural explanations which are going to be given in the paragraph below, there are two possible reasons for this finding. The first reason is that the number of computer forensic investigators and analysts is limited. Thus, universities cannot have relevant courses due to monetary difficulty. The second reason is that on-the-job training provides a good opportunity for junior computer forensic workers to learn and understand the latest techniques and cases.

In Question 22, seven experts agreed that there are certain methods to train computer forensic investigators. In addition, this infers that there is no standard training method in Taiwan at this moment. Four out of these seven experts, including one academic researcher and three computer forensic practitioners, described that the computer forensic investigators are normally sent out overseas for the training courses.

Cultural explanations can be provided for the findings of Question 17, 19, 21, and 22. In here, these questions are discussed as a whole, since they all have similar cultural explanations. There is no standard computer forensic exam for experts within this field, and there is no official and authorized organization to certify computer forensic experts either. Moreover, instead of a systematic training method, Delphi experts described that there are different ways to train computer forensic experts. For example, on-the-job training for computer forensic investigators is one of the methods within this field. Three computer forensic practitioners further stated that sending computer forensic workers overseas for foreign computer forensic exams and vendor-based training courses is a common way to train computer forensic experts.

These phenomena can be explained by two cultural reasons. The first reason is that Taiwanese culture tends to avoid any possible uncertainty. Since the current methods are acceptable and working, there is no need to set up a national standard. Too many unpredictable factors may occur if the current situations and methods are changed. In addition, this infers that Taiwanese culture cares only about the existence of a solution, rather than the quality of the solution. The second reason is that Taiwanese culture realizes that the development of the applications of science is not strong. Thus, computer forensic investigators are usually sent overseas for advanced training. In summary, the proposed cultural accounts can perfectly explain the findings of Question 17, 19, 21, and 22.

The two cultural reasons match that provided by Hofstede (1980) and the concepts of Confucianism (Jingpan 1990; Ho 1991) respectively. According to Hofstede, uncertainty avoidance plays an important role in Taiwanese culture. Moreover, like the discussion of Delphi Question 1, 2, and 3, it is realized that Confucianism does not emphasize the value of science (Western scientific values). In short, the cultural findings of these four Delphi questions (Question 17, 19, 21, and 22) are trustworthy.

The findings in Question 23 can be mainly classified into five categories. There is no explicit agreement for this question. Various opinions are found in this question. Thus, Question 8 of the Round Two Delphi survey is created to seek for the Delphi consensus. Fortunately, 80% agreement is achieved, and the consensus shows eight experts agreed that it at least needs one year to train a computer forensic investigator. The phenomenon discovered by this question can be perfectly explained when combining the Australian and Taiwanese findings of this question. Thus, the cultural interpretation is discussed in Section 6.4.

5.2.3.4 Law Dimension

Four questions, Question 35 to 38, were designed for this dimension in the Round One Delphi questionnaire. The agreement of Question 36, 37, and 38 were 90%, 70%, and 80% correspondingly. Every question reached the consensus except the Question 35, which became Question 11 in the Round Two Delphi questionnaire. Fortunately, Question 11 in the Round Two Delphi questionnaire reached 90% agreement. In summary, four questions in this dimension reached the consensus after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questions of this dimension are listed below.

- ***Question 35: In your experience, do courts give a high or low weighting to digital evidence in your country?***
    - ***Derivative Question (Question 11 in the Round Two Delphi Questionnaire): In Taiwan, although the court cannot overlook the importance of digital evidence, the court normally gives a low weighting to digital evidence. The only exception is that the digital evidence is valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 36: Do you know of any difficulties caused by using digital evidence in court? If "SO", what has been the major reason for this?***
- ***Question 37: Based on your knowledge, is it the suspect's obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If "YES", Can you provide the name of the law?***

- ***Question 38: Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If "SO", does this affect the attitude of computer forensic investigators to perform investigations? If "YES", can you briefly explain?***

The finding in Question 35 shows that six experts agreed that the court give a low weighting to digital evidence. This means that the agreement of Question 35 was 60%, and did not reach the consensus. This is because two experts, including one academic researcher and one computer forensic practitioner, stated that the court gives a high weighting to digital evidence, and two computer forensic practitioners claimed that the weighting of digital evidence depends on the type of case. If it is a computer crime, the weighting of digital evidence is considered high. On the contrary, if it is a traditional case, the weighting of digital evidence is considered low. Unlike traditional forensic evidence (e.g. DNA and fingerprint), the status of digital evidence is variable in a court of law. Fortunately, three experts change their minds in Question 11 of the Round Two Delphi survey. This means 90% agreement was achieved for Question 11 of the Round Two Delphi questionnaire.

90% agreement was achieved for Question 36. There are many difficulties in presenting digital evidence in a court. The major problem is that the members of the court do not entirely understand the concept of digital evidence.

The findings of Question 35 and 36 can be explained by an understanding of the nature of Taiwanese culture. The typical concepts of Taiwanese culture are: 1. *if I cannot solve my own problem, how could I help to solve other people's problems?*, and 2. *if I cannot solve current problem, how could I solve the problems in the future?*. This infers that uncertainty avoidance plays an important role in Taiwanese culture. Moreover, this concept is also proved by Hofstede (1980).

People in Taiwan are normally concerned with their own problems first, and do not care about other issues. In this manner, it is comprehensible that the members of the court normally do not have enough understanding about digital evidence, and usually give a low weighting to digital evidence. This also causes a major problem when presenting digital evidence in a court.

In Question 37, seven experts, including two academic researcher and five computer forensic practitioners, agreed that there is no law which asks the suspect to provide digital evidence as his or her obligation. One of them further stated that it is prosecutor's responsibility to provide relevant evidence, including digital evidence. The above phenomena are understandable by understanding the thinking of Taiwanese, the behaviours of Taiwanese, and the nature of Taiwanese culture. It is common for people to try any possible means and/or excuses to avoid serious consequences and/or penalties, and there is no exception for people in Taiwan. The major concept to design the Taiwanese laws, including criminal law and civil law, is to prevent the above situation.

Discussion of Taiwanese laws can be found in Poh-Ling (1997). Thus, these laws neither ask a plaintiff and/or a defendant to provide relevant evidence, including digital evidence, as their obligations, nor request two parties to exchange relevant data before the trial. It is the prosecutor's responsibility to seek the relevant evidence, including digital evidence. In summary, Taiwanese laws are designed to overcome the presumed evil nature of humanity.

80% agreement was achieved for Question 38. Two experts, including one academic researcher and one computer forensic practitioner, did not agree with Question 38. In addition, three out of the other eight experts further stated that the attitudes of computer forensic investigators are affected if the development of computer forensic technology is beyond the development of the current law. This phenomenon is caused by the following reason. It is common for the law to be legislated after related incidents (Hojring 2002). Thus, it is understandable that the development of computer forensics is beyond the development of relevant laws. The gap between the latest technology and relevant legislation has always existed. In addition, the interesting finding of this question is that three Delphi respondents further stated that the attitudes of computer forensic investigators are affected by the imperfection of legislation. This is because the nature of Taiwanese culture believes more in collectivism than individualism. People in Taiwan normally seek their identification within a group. This infers that they are more easily affected by outside factors, and their attitudes are changed by these outside variables as well. An individual tends to agree with the conclusion agreed to by others, and to follow the decision made by others as well. This argument was confirmed by Hofstede's work (1980) as well. According to Hofstede, Taiwanese culture is built on

collectivism and interdependence. Therefore, it is explainable that three experts claimed the attitudes of computer forensic investigators are affected by the incompletion of legislation.

5.2.3.5 Personal Preferences and Skills Dimension

There are five questions in this dimension, and they are Question 24, 25, 26, 39, and 40 in the Round One Delphi questionnaire. The agreement of Question 24, 26, 39, and 40 were 90%, 70%, 70%, and 90% respectively. On the contrary, Question 25 did not reach the consensus and became Question 9 in the Round Two Delphi questionnaire. Fortunately, Question 9 in the Round Two Delphi questionnaire reached 80% agreement. In short, Delphi consensuses for these five questions were made after two rounds of Delphi survey. The original questions in the Round One Delphi questionnaire and the derivative questions in the Round Two Delphi questionnaire of this dimension are listed below.

- ***Question 24: What is your opinion concerning the importance of hash functions in the field of computer forensics?***
- ***Question 25: Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?***
    - ***Derivative Question (Question 9 in the Round Two Delphi Questionnaire): The collision of hash function has influence on computer forensics. The influence may include: reliability of digital evidence, and more difficult to perform a computer forensic investigation. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?)***
- ***Question 26: Based on your knowledge, what are the countermeasures within computer forensics to the collisions of hash functions?***
- ***Question 39: As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?***
- ***Question 40: As a computer forensic professional, do you use any type of encryption tools for the data in your work?***

In Question 24, Delphi respondents believed in the importance of the hash function. Only one expert stated that he is not familiar with this issue. The other nine experts, with academic backgrounds and practical experience, agreed with this question. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. In the field of computer forensics, the purpose of hash function is to ensure the integrity of digital evidence, which is the essential requirement of digital evidence. This statement can also be proved by the findings of Question 8 in the Round One Delphi questionnaire and Question 3 in the Round Two Delphi questionnaire. In short, seeking the integrity of digital evidence is necessary in the field of computer forensics. Thus, the importance of hash function is not a debated issue in this field.

The findings in Question 25 show that six experts agreed that the collisions of hash functions have impact on digital evidence. This means that the agreement of Question 25 is 60%, and did not reach the Delphi consensus. Three out these six experts are academic researchers, and the other three experts are computer forensic practitioner. Fortunately, two experts changed their minds in Question 9 of the Round Two Delphi survey. One of these two experts is academic researcher, and the other one is computer forensic practitioner. This means that Question 9 of the Round Two Delphi questionnaire reached 80% agreement. The observed situation can be explained by the nature of Taiwanese culture. People in Taiwan are used to seek for the absolute truth and unambiguous answer. They believe there is only one answer for a problem. This concept not only was formed while they studied in the elementary school, but also is supported by Hofstede (1980) who stated that "*The search is for ultimate, absolute truths and values.*" is a typical trait of Taiwanese culture. Thus, it is understandable that experts still think that the collisions of hash functions have impacts on applications of computer forensics although the possibilities of the collisions of hash functions are very low.

70% agreement was achieved for Question 26. Seven experts, who agreed with this question, consisted of three academic researchers and four computer forensic practitioners. They mainly stated that using more than one hash functions is a well-accepted method for the current situation. The findings of this question show that some values within the field of computer forensics are beyond the influence of culture. Within the field of computer forensics, using several hash functions is an acceptable method to

ensure the integrity of digital evidence since there is no better solution at this moment. In this case, computer forensic investigators can claim that any uncertainty of the digital evidence is removed. From the scientific viewpoint, the integrity of digital evidence is completely ensured. In conclusion, it is understandable that technical skills are not affected by different cultures.

In Question 39, seven Delphi experts stated that they do use data wiping tools. This means 70% agreement was achieved for this question. The seven Delphi respondents consisted of three academic researchers, and four computer forensic practitioners. In addition, one out of four computer forensic practitioners has legal background.

90% Agreement was achieved for the Question 40. Only one academic researcher stated that he does not use data encryption tools. The other nine Delphi experts agreed that they do use data encryption tools.

Question 39 and 40 can be explained together by the typical Taiwanese cultural attitude. As computer forensic experts, most of they use data wiping tools and data encryption tools for unnecessary data and confidential data respectively. This situation can be explained by two reasons. The first reason is that the respondents are experts with computer forensic expertise. Thus, they know the importance of protecting critical data. After all, their jobs are dealing with significant digital data. The second reason is that the competition is so aggressive in Taiwan, since the population is greater than the available resources. Hofstede (1980) also stated that higher anxiety and stress are two typical features of strong uncertainty avoidance society, and Taiwan based on his classification is strong uncertainty avoidance. Consequently, an individual needs to learn how to contend in most circumstances in order to be the winner, to discover how to win so as to obtain more resources, and to find out a way to protect himself or herself from unpredicted scenarios. This explains the uses of data wiping tools and data encryption tools. Using data wiping tools and data encryption tools is a way for respondents to protect their privacies and properties. In summary, the Delphi respondents use data wiping tools and data encryption tools for two reasons: 1. professional expertise, and 2. special living experience and background.

5.2.3.6 Cross Questions

Interesting phenomena are found after the interpretations of 40 Delphi questions. It is discovered that there are some corroborations between different questions. In this case, the validity of these findings is further improved by these cross-question corroborations. In this section, these corroborations are going to be listed and discussed.

Comparing the findings of Question 1 and 2 shows the typical nature of Taiwanese culture. Delphi consensus for Question 1 shows that Taiwanese government realizes the importance of computer forensics. However, Delphi respondents in Question 2 generally agreed that more attentions should be put in the field of computer forensics. In summary, the Taiwanese government comprehends the value of computer forensics, but does not put enough attentions on this issue. These two conflicting findings corroborate the standpoint proposed by this thesis which describes that Taiwanese culture tends to focus on short-term objectives, and is likely to ignore plans for the future (Hofstede 1980). In this case, it is not surprising that the essence of the problem is sometimes missed.

The findings of the following 11 Questions (Question 5, 7, 13, 15, 17, 19, 22, 30, 35, 36, and 38) respond the results of Question 2. These eleven questions contain various perspectives (e.g. the technical perspective, the legal perspective, and the educational perspective), and list the current problems within the field of computer forensics in Taiwan. Thus, it is understandable that the results of Question 2 show that most of Delphi respondents do not satisfy with the current development of computer forensics. In addition, the discoveries of Question 30 are able to support the outcomes of Question 36, and vice versa. These two questions both point out that members of the court do not entirely understand the characteristics of digital evidence are a barrier for performing computer forensics.

After finishing the Delphi survey, it is realized that the findings of 10 questions (Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31) are beyond the cultural influence. This is because the core concepts of these 10 questions are global values, which are not affected by different cultures. For example, culture may affect the way people think about addition, but it is not going to change the result of the addition (e.g. 1+1=2). In addition, the discoveries of Question 12 further respond to the results of Question 31, and vice versa. The findings of these two questions agreed that using multiple methods

and/or data sources is a widespread method for carrying a legal investigation. In summary, the Delphi survey in this research has discovered that there are consistent and independent values within the field of computer forensics.

The findings of Question 5, 17, 19, and 22 lead to a single deduction. Instead of national standard, alternative methods are currently used for computer forensic SOPs, forming, certifying, and training a computer forensic expert. The findings of these four questions are identical, and show that lack of a national standard is currently a serious issue within the field of computer forensics in Taiwan.

In Question 3, 5, 9, 10, 11, 14, 17, 19, 21, 22, 25, 26, 28, and 29, the answers, provided by the only Delphi expert with legal background, reveal an interesting viewpoint, which corroborate the findings of Question 35 and 36. The Delphi respondent with legal background stated either he is not familiar with the previous 14 questions or these 14 questions are beyond his specialism. Combining his answers and his legal background proves the consensus of Question 36, and the results of Question 35. The validities of the findings of these two questions are further confirmed. In addition, the findings of question 36 give a reasonable explanation for the Delphi consensus of Question 35. In Question 36, Delphi respondents agreed that the major problem encountered when using digital evidence in the court is that the members of the court do not entirely understand the digital evidence. This situation explains why a low weighting is normally given to digital evidence (confirmed by Question 35).

5.2.4 Summary of Section 5.2

Section 5.2 is classified into three sub-sections, which discusses the experts, results, and cultural interpretations of the Taiwanese Delphi survey respectively. Section 5.2.1 anonymously provides the basic understanding of ten Taiwanese Delphi respondents, which consist of five academic researchers, one legal expert, and four computer forensic practitioners. This infers that the answers and opinions provided by them are compelling and trustworthy, and also confirms the confidentiality of their identities. In addition, Section 5.2.2 lists the findings of Taiwanese Delphi survey, and these findings are showed by five dimensions. Lastly, the cultural interpretations for the Delphi results are listed in Section 5.2.3, and these cultural interpretations are presented in five dimensions as well. These cultural interpretations respond to the research question of

this thesis, and demonstrate the relationship between computer forensics and culture. In addition, Section 5.2.3.6 further builds the relationship between different Delphi questions. For example, the relationship between Question 1 and 2 validates the existence of cross-questions relationship.

In conclusion, according to a cultural interpretation, it is not surprising why Taiwanese deal with computer forensic issues in specific ways. Culture is thus considered one of the most important factors which can affect the applications of computer forensics.

5.3 Case Study

Thorough explanations of the concept of case study can be found in Section 3.6. Five dimensions, created in this thesis, are used as criteria into case study to examine the latest computer forensic situation in Taiwan. The five dimensions are: *Current Situation Dimension*, *Policy and Organization Dimension*, *Education Dimension*, *Law Dimension*, and *Personal Preference and Skill Dimension*. Unlike the Delphi method, the case study utilizes any other valuable information regardless of the sources. Data from websites, newspapers, memorandums, and personal interviews are useful and helpful for this case study.

This section presents two Taiwanese case studies without revealing the names of two case study respondents and their organizations. In Section 5.3.1 the first Taiwanese case study is introduced, and Section 5.3.2 describes the second Taiwanese case study. In addition, Section 5.3.3 compares the two Taiwanese case studies.

5.3.1 First Taiwanese Case Study

In this thesis, a law enforcement agency in Taipei is the subject of the first Taiwanese case study. According to the experiences learned from the Taiwanese Delphi survey, computer forensic experts in Taiwan mainly come from police system and academia. In this case, it is reasonable for this thesis to choose a law enforcement agency as the organization for this case study. In addition, this situation further infers that the computer forensic investigators within law enforcement agencies are perfect candidates for this research. Lastly, the quality of the case study questionnaire was discussed in Section 3.6.6.2 and can be applied here.

5.3.1.1 Findings of the First Case Study

This section shows the input provided by Taiwanese Case Study Expert (TCSE) 1. The findings are listed in five dimensions. The first four questions (Question 1 to 4) belong to the Current Situation Dimension. Question 5 and 6 belong to the Policy and Organization Dimension. In the Education Dimension, there are three questions, and they are Question 7, 8, and 9. In addition, the Law Dimension consists of two questions, which are Question 10 and 11. Lastly, Question 12 and 13 are listed in the Personal Preference and Skill Dimension.

In this case study, case study questions were asked in order to draw out TCSE 1's interpretation of the current situation of computer forensics in Taiwan. TCSE 1 was encouraged to provide additional information during the interview.

5.3.1.1.1 Current Situation Dimension

Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.

TCSE 1: I admit the importance of SOPs. Nevertheless, there are no SOPs in my organization at this moment. My organization is trying to define SOPs which are suitable for the situations in Taiwan. My organization already has research results from academic researchers. The results are helpful for pointing out the correct direction for building SOPs. Moreover, my organization is trying to obtain the relevant SOPs from the law enforcement organizations of the United States of America as guidelines.

Question 2: Generally speaking, there are two common means of obtaining digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability of digital evidence in court?

TCSE 1: I have encountered both situations. I did seize computers at crime scenes, but computers are sometimes sent to me for further analysis by traditional investigators. I agree that differences exist between these two means. If I can collect digital evidence by myself, I will follow existing guidelines, regulations, and procedures for identifying and collecting digital evidence. However, it is common to discover errors in the seized digital evidence if the digital evidence is transferred from other officers or departments. In this case, it is very hard to perform computer forensic analysis on the collected digital evidence. In the worst case, the computer forensic analysis may never be done.

Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?

TCSE 1: At this moment, there are only six experts working in my organization. It is impossible for six experts to deal with the computer forensic needs for a whole country, which contains around 23 million people. Thus, my organization normally deals with national and serious digital crimes.

Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?

TCSE 1: There are two ways to recruit new staffs. The first one is to choose new staffs from the people who pass a particular exam. The purpose of this exam is to allow people to work in my Branch. The second method is to choose new staffs from colleagues, having computer backgrounds and skills, in other departments.

5.3.1.1.2 Policy and Organization Dimension

Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.

TCSE 1: I agree that government policies are able to affect the development of computer forensics. If the corresponding policies or legislation are not well-defined, the role of computer forensics is ambiguous. For example, the computer forensic analyst has made certain discoveries after examining the digital evidence. However, these discoveries may not be suitable to be presented at a court because the court does not admit the digital evidence. This is because that the government does not have well-defined policies or legislation for the role of digital evidence. Unfortunately, I can do nothing to change this situation. My job is to ensure the correctness of digital evidence.

Question 6: In your country, what organisations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.

TCSE 1: From my understanding, CIB (Criminal Investigation Bureau 2007) has the ability to cope with computer forensic tasks. Moreover, there are some military organizations which have the ability to deal with computer forensic issues. However, I do know which private companies have such ability, since my organization does not have close contacts with private companies.

5.3.1.1.3 Education Dimension

Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?

TCSE 1: I started this job before the cyber forensics laboratory was built. Thus, I did not attend any exams or tests. My on-the-job training mainly is official courses for new equipment, including computer forensic hardware and software. I am usually sent overseas to attend computer forensic courses and/or conferences. I have done this job for around two years.

Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?

TCSE 1: More precise methods are used to train new staff. It is different from the way that I encountered, since I did not attend any exams or tests. In addition, my organization is preparing a standard training program.

Question 9: In your country, are there any tertiary-level courses that teach computer forensics?

TCSE 1: From my understanding, CPU teaches computer forensic courses. This is understandable since CPU plays a different role to usual universities. I am not sure about the situation in other universities.

5.3.1.1.4 Law Dimension

Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?

B) In your own experience, what is the level of legal knowledge that computer forensic analysts have?

TCSE 1: A) I agree with this statement. Because the ultimate purpose of computer forensics is to present digital evidence to a court, it is meaningful for computer forensic investigators to understand law relevant issues. This also infers that the development of computer forensics is based on the usage of digital evidence within a court.

B) Taking me as an example, I slightly understand the relevant law since I spend most of my time on my job. In addition, I believe this situation is hard to change in the near future, and there is nothing I can do to change this situation. Changing this situation is beyond my ability and job.

Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?

B) In your own experience, what is the level of computer forensic knowledge that members of the court have?

TCSE 1: A) I agree with the statement, since I believe digital evidence will play an important role in the near future. This is mainly because of the involvement of electronic equipment.

B) In Taiwan, members of the court do not completely understand the features of the digital evidence, nor entirely comprehend the issues of computer forensics. I believe this situation can only be changed and improved by cross-organization cooperation. This issue is beyond my ability to influence.

5.3.1.1.5 Personal Preference and Skill Dimension

Question 12: As a computer forensic professional, do you use data wiping tools and/or data encryption tools for your data?

TCSE 1: Yes, I use both tools for my personal data in most conditions.

Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?

TCSE 1: My organization provides funds annually for educational and training purposes. There is no in-house educational or training program. The major way is to send computer forensic investigators overseas to attend critical training courses. In addition, computer forensic investigators are encouraged to attend the exams provided by famous computer forensic organizations and manufacturers.

5.3.1.2 Interpretations of the First Case Study Findings

TCSE 1 provided his opinions based on his professional experiences. In this section, the cultural interpretations of his opinions are provided. These explanations are made based on the five dimensions in order to clearly understand the computer forensic conditions.

5.3.1.2.1 Current Situation Dimension

There are four questions in total in this dimension, and they are Question 1, 2, 3, and 4 of the case study questionnaire. These four questions are listed as follows.

- ***Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.***
- ***Question 2: Generally speaking, there are two common means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?***
- ***Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?***
- ***Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?***

In Question 1, TCSE 1 realized the importance of computer forensic SOPs, but also agreed that there are currently no computer forensic SOPs in his organization. He stated that his organization is trying to define its own SOPs. This situation can be explained by the nature of Taiwanese culture. Short-term objectives normally obtain more attention than long-term objectives. This indicates Taiwanese culture tends to focus on the existence of a solution rather than the quality of a solution. If there is currently an acceptable solution, changing or improving this solution is not the top priority. Change or improvement only takes place when there is an urgent need. This argument is

corroborated by Hofstede (1980). In his work, he confirmed the relationship between Taiwanese culture and strong uncertainty avoidance.

In Question 2, the computer is sometimes seized by computer forensic experts, and is occasionally seized by non-technical individuals (e.g. local police officer). TCSE 1 agreed that it is a better choice for him to do the seizure himself, since it is common to discover errors on the seized digital evidence when processed by other people and/or organizations. This phenomenon is understandable since Taiwanese culture puts more emphasis on short-term objectives. This standpoint is proved by Hofstede (1980) as well. He described that Taiwanese culture is strong uncertainty avoidance. This infers that long-term objectives are not usually discussed in Taiwanese culture. At this moment, computer forensics is only an interesting topic for a small group of people (e.g. academic researchers and computer forensic investigators in corresponding government organizations). This means that the majority of police officers do not understand the issues within computer forensics. However, with the increasing number of digital crimes, the concept of computer forensics may become more popularized. Instead of asking every police officer to learn advanced computer forensic skills, they at least need to know what they can do and what they cannot do to the relevant digital equipments, and how to maintain the integrity of digital evidence. Unfortunately, TCSE 1 demonstrates most of police officers do not have enough understanding of computer forensics.

In Question 3, TCSE 1 did not think that the number of computer forensic investigators in his organization is enough. This finding not only indicates that there are some values within the field of computer forensics beyond the influence of culture, but also responds to the discoveries of Delphi Question 30. In reality, financial support from government for computer forensic issues is always limited, since computer forensics is only one out of many concerns of the Taiwanese government. For example, the Taiwanese government also needs to sustain the manpower for power stations and other facilities. Consequently, the shortage of computer forensic workers is understandable, and this situation is caused by financial reasons rather than a cultural influence.

In Question 4, TCSE 1 stated that there are two different ways for recruiting new computer forensic employees in his organization. The first way is using specific exams for recruiting future employees, and the second way is to transfer employees from other

departments (e.g. computer security department) to the computer forensic department. The interesting phenomenon is only found for the first recruiting method since the second recruiting method is a widespread one in the rest of the world. A cultural interpretation can be provided for the first recruiting method. Attending exams is a traditional method, which has been very popular in Chinese culture, for thousand years (Haifeng 2006). Since Taiwanese culture is a branch of Chinese culture, it is not surprising that attending exams has become a major way for recruiting new staff in TCSE 1's organization. In Taiwanese culture, exams are used to estimate the ability and the value of an individual. The expertise and the ability of an individual to think scientifically are not the first concern when recruiting employees.

5.3.1.2.2 Policy and Organization Dimension

There are two questions, Question 5 and 6 of the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.***
- ***Question 6: In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.***

In Question 5, TCSE 1 stated that the government policies on computer forensics indeed affect the development of computer forensics, and the government should pay more attention to the computer forensic policies. This is because well-defined policies are capable of preventing possible disputes in the future. In this case, computer forensic investigators and/or analysts have clear rules to follow, and possible ambiguities can be ruled out. Avoiding uncertainty is a well-accepted concept in Taiwanese culture. In addition, TCSE 1 provided an interesting standpoint describing that he can do nothing to change this situation since he is only a computer forensic analyst. His work focuses on providing valid digital evidence rather than offering opinions or making decisions on computer forensic policies.

The findings of this question can be explained by the nature of Taiwanese culture. Since Taiwanese culture focuses more on short-term objectives rather than long-term goals, this reason explains why Taiwanese government is not keen to set up new legislation. In this case, it is not surprising that the development of new laws cannot keep up with the developments of computer forensics. In addition, TCSE 1 agreed that the government policies of computer forensics indeed affect the developments of computer forensics. This is because the nature of Taiwanese culture focuses on more collectivism rather than individualism. This means that people in Taiwan are essentially seeking the identification within a group rather than as individuals. Thus, the behaviours and attitudes of people are more easily affected by outside factors and variables. An individual tends to agree the conclusion agreed by others, and to follow the decision made by others as well. Lastly, the answer of TCSE 1 shows an interesting but typical attitude of Taiwanese culture. He expressed that he can do nothing to improve that current situations within computer forensic policies, since he only works as a computer forensic investigator. The development of computer forensic policies is not his responsibility, and is beyond his ability. This is because people in Taiwan believe that '*if I cannot solve my own problem, how could I help to solve other people's problems?*'. This indicates that they put primary emphasis on their own work and do not have much concern about other people's work. In summary, the above cultural standpoints explain the responses of TCSE 1. In addition, the previous three cultural interpretations can be found in and are supported by Hofstede's work (1980). According to Hofstede, collectivism, group, uncertainty avoidance are three characteristics in Taiwanese culture.

In Question 6, only central (federal-level) government organizations (e.g. MJIB and CIB), and some military organizations have the ability to deal with computer forensic issues. There is no local (state-level) computer forensic laboratory. This phenomenon demonstrates that the Taiwanese government should place more attention on the field of computer forensics. It is believed that the importance, and the development of computer forensics are not completely understood by the Taiwanese government, since it is impossible to ask the employees of central (federal-level) computer forensic organizations to deal with every digital incident occurred in Taiwan. With no doubt, this shows that avoiding uncertainty is part of Taiwanese culture. As long as a solution exists, the quality of the solution is not going to be discussed. Unnecessary changes should be avoided. This means that the essence of the issue is sometimes overlooked. In

addition, it is obvious that TCSE 1's organization does not have good relationships with private companies, which have computer forensic ability, since TCSE 1 is not familiar with the current situations outside the government organizations. This situation reflects an aspect of Taiwanese culture. People in Taiwan usually consider their own problems first, and sometimes care only about their own issues. Thus, understanding other person's and/or organization's issues is not the top priority in Taiwanese culture. In addition, the cultural interpretations of this question are deeply related to the concept of uncertainty avoidance which was proposed by Hofstede (1980). Based on the research of Hofstede, Taiwanese culture has strong uncertainty avoidance.

5.3.1.2.3 Education Dimension

There are three questions, Question 7, 8, and 9 of the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?***
- ***Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?***
- ***Question 9: In your country, are there any tertiary-level courses that teach computer forensics?***

The findings of Question 7 and 8 can be explained together. There were no requirements for TCSE 1 when he started his current job around two years ago. However, there are several types of on-the-job training for TCSE 1, and the major on-the-job training is official courses for new equipment, including computer forensic hardware and software. TCSE 1 further stated that he is usually sent overseas to attend computer forensic courses and/or conferences. In addition, unlike his own experience, TCSE 1 agreed that current method to train new employees are improving and changing.

The findings of Question 7 and 8 can be explained jointly by understanding the nature of Taiwanese culture. TCSE 1 agreed that the training methods for new employees are improving. This is because Taiwanese culture tends to seek the unambiguous answer. People in Taiwan have sought exact and unambiguous answer since elementary school, and they are always told that there is only one correct answer for a question. This argument is supported by Hofstede (1980) as well. In his research, he discovered the same standpoint as used in this thesis. In this case, it is understandable that TCSE 1's organization is actually trying to build a standard training program.

In addition, sending computer forensic investigators overseas for training purposes shows that Taiwanese culture does not put an emphasis on science, and usually follows the lead of Western countries in the field of science. This is because Confucianism, which does not place attention on the value of science (Western scientific values), has affected Chinese culture, which is the source of Taiwanese culture, for thousand years (Jingpan 1990; Ho 1991). Therefore, it is not surprising that Taiwanese culture does not put emphasis on science. In summary, the answers of Question 7 and 8 are actually affected by the uniqueness of Taiwanese culture.

In Question 9, TCSE 1 stated that computer forensic courses are taught in CPU. This is understandable due to the special role of CPU. However, he is not familiar with the situations within other universities. In fact, there are also other universities, such as Tamkang University (Tamkang University 2007) and National Kaohsiung First University of Science and Technology (National Kaohsiung First University of Science and Technology 2007), having computer forensic courses. The phenomenon is believed to be caused by a cultural explanation. At this moment, only a particular group of people realize the importance of computer forensics in Taiwan, and computer forensics does not obtain enough attentions. Nevertheless, Pollitt (1995a) stated that the need for computer forensics will grow dramatically. This means the need for the computer forensic experts is going to increase as well. However, there is obviously no proper preparation for the development of the future experts. This is because people in Taiwan normally face a problem when they actually encounter the problem. They usually do not consider potential solutions for things or events which have not actually occurred. This perspective can be found in Hofstede's research results (1980). This indicates that the cultural interpretations of this question are supported by discoveries of Hofstede's work.

5.3.1.2.4 Law Dimension

There are two questions in this dimension, and they are Question 10 and 11 of the case study questionnaire. These two questions are listed as follows.

- ***Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?***

  B) In your own experience, what is the level of legal knowledge that forensic analysts have?
- ***Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?***

  B) In your own experience, what is the level of legal knowledge that members of the court have?

The findings of Question 10 and 11 can be explained jointly by understanding the nature of Taiwanese culture. From the standpoint of TCSE 1, the level of understanding between computer forensic investigators and members of the court is not deep enough. The findings of legal and technical issues of question 10 show that computer forensic investigators need to spend some additional effort on understanding legal issues, and the results of question 11 point out that members of the court should place greater attention to the relevant computer forensic issues as well. However, computer forensic investigators normally do not have adequate time to learn legal issues. Limited numbers of computer forensic investigators are in charge of investigations into the digital crimes of the entire country. For example, TCSE 1's organization has only 6 computer forensic investigators at this moment. In contrast, members of the court encounter similar situation. They have excellent legal knowledge, but do not have expertise for the technical issues which are associated with computer forensics. TCSE 1 knows that the above situations are currently a problem, and he also stated that cross-organizations cooperation is a way to solve this situation. Unfortunately, he expressed that the developing cooperation is beyond his ability, and is not part of his job.

A typical Taiwanese cultural attitude can provide a rational explanation for the findings of Question 10 and 11. This is because people in Taiwan believe that '*if I can not solve my own problem, how could I help to solve other people's problems?*'. This means

people in Taiwan are used to focus on their own issues rather than other irrelevant issues. They are only responsible for their work. This viewpoint is corroborated by Hofstede (1980). In his work, he used the term, '*strong uncertainty avoidance*', to describe the characteristic of Taiwanese culture. Hofstede's term has the same meaning as the cultural interpretation of these two questions. In this case, the core of the problem (e.g. mutual understanding between computer forensic investigators and members of the court) is likely to be overlooked. In short, the above cultural standpoints explain the responses of TCSE 1.

5.3.1.2.5 Personal Preference and Skill Dimension

There are two questions in this dimension, and they are Question 12 and 13 of the case study questionnaire. These two questions are listed as follows.

- ***Question 12: As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?***
- ***Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?***

In Question 12, TCSE 1 stated that he uses data wiping tools and data encryption tools in most situations. There is a rational cultural explanation for the findings of this question. In Taiwan, the population is larger than available resources. Society is competitive and everyone not only needs to work hard in order to gain good results in all aspects of life, but also requires to learn how to protect himself or herself, and their property, well. This argument is discussed in Delphi Question 28. Thus, the use of data wiping tools and/or data encryption tools is understandable, since it is a useful way to protect one's privacy and property.

In Question 13, the findings show that the development of computer forensics within TCSE 1's organization is continuous. The importance of this development is acknowledged. In most cases, computer forensic investigators are sent overseas for systematic training, such as vendor-based training courses, and are encouraged to attend exams provided by famous computer forensic organizations. However, there is no formal in-house course.

These situations can be explained by the following cultural interpretations. The first cultural explanation is that Taiwanese culture does not consider science a serious subject. This is because with Confucianism (Jingpan 1990; Ho 1991; Slay 2000b) there is no focus on scientific development. In this thesis, the scientific development means Western scientific values. Unfortunately, Confucianism is the major educational philosophy accepted by Taiwanese culture. Thus, it is not surprising that there is no in-house course within the field of computer forensics. In addition, the second cultural interpretation is that Taiwanese culture is used to follow the lead of Western science. This inference is discussed in the Delphi Question 1, 2, and 3. Therefore, it is understandable that computer forensic experts are normally sent overseas for advanced training and/or qualifications.

5.3.1.2.6 Cross Questions

In this section, the researcher tries to establish any possible relationship between the case study questions. This section builds the relationship between Question 7 and 8. Although findings of Question 7 cannot directly prove the results of Question 8, combining the findings of Question 7 and 8 it is possible to conclude that improvements in computer forensic training are actually occurring in TCSE 1's organization. In Question 7, TCSE 1 stated that there is no technical prerequisite or qualification for him when he started his current job. In addition, the findings of Question 8 show that there are other methods for training a computer forensic investigator at present. Within TCSE 1's organization, computer forensic workers know the importance of certifications, educational programs, and training courses, and are actually changing and improving the situations. In summary, combining the answers to Question 7 and 8 shows that improvements in computer forensic training are occurring.

5.3.2 Second Taiwanese Case Study

The basic understanding for the second Taiwanese case study is introduced so as to ensure the quality of this case study. In order to satisfy this need, three quality factors of this case study need to be examined. They are quality of the case study organization, participant, and questionnaire.

A law enforcement agency is a suitable choice for the second Taiwanese case study due to the uniqueness of computer forensics. This topic is discussed in several groupings, such as academia and law enforcement. This situation further means that computer forensic investigators working for the law enforcement agency are suitable candidates for this research because of their professional experiences. Lastly, the quality of a case study questionnaire is discussed in Section 3.6.6.2. In summary, the quality of the second Taiwanese case study is good when compared to the stated quality criteria.

5.3.2.1 Findings of the Second Case Study

TCSE 2 provided his professional opinions for the second case study interview, and his opinions are listed in this section. By understanding his standpoints, the latest situations of computer forensics in Taiwan are revealed. In addition, the thirteen case study questions are listed in five dimensions created by this thesis. The first four questions (Question 1 to Question 4) belong to the Current Situation Dimension. Question 5 and 6 belong to the Policy and Organization Dimension. In the Education Dimension, there are three questions, and they are Question 7, 8, and 9. In addition, the Law Dimension consists of two questions, which are Question 10 and 11. Lastly, Question 12 and 13 are listed in the Personal Preference and Skill Dimension.

In the case study interview, 13 questions were asked in order to draw out TCSE 2's interpretation of the current situation of computer forensics in Taiwan. TCSE 2 was encouraged to provide additional information during the interview.

5.3.2.1.1 Current Situation Dimension

Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.

TCSE 2: My colleagues and I realize the importance of SOPs. My organization has research results from academic researchers and indeed utilizes these results to clarify the major issues in collecting and analysing digital evidence. However, there are no precise SOPs in my organization.

Question 2: Generally speaking, there are two common means of obtaining digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?

TCSE 2: I have encountered both situations. Sometimes I collect the digital evidence, and seize the computer myself. I agree that there are differences between these two means. If the evidence is collected by a computer forensic specialist, it is helpful for the integrity and trustworthiness of digital evidence. This can prevent other non-technical investigators damaging digital evidence by incorrect actions or procedures.

Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?

TCSE 2: I do not think manpower is enough to deal with the computer forensic needs of the jurisdictional scope. We can only deal with the cases with the highest priority.

Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?

TCSE 2: There are two ways to recruit new staffs. The first and the major method is to choose new staff from the people who pass the particular exam. The purpose of this exam is to allow people to work in my organization. The second method is to choose new staff from colleagues with computer backgrounds.

5.3.2.1.2 Policy and Organization Dimension

Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.

TCSE 2: The answer to this question is affirmative. A well-defined law and system can prevent possible disputes of digital evidence from occurring in the future. In this manner, collected digital evidence is trustworthy since it is processed based on the regulations of law. However, the court does not give a high weighting to digital evidence at this moment. The importance of digital evidence is sometimes overlooked. Unfortunately, this situation is beyond my ability, and the only thing I can do is to provide correct and valuable digital evidence. After all, I am only a computer forensic analyst.

Question 6: In your country, what organisations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.

TCSE 2: In Taiwan, MJIB, and CIB are two government organizations, which can deal with computer forensic issues. I do not think that private companies need to deal with computer forensic problems although they may have adequate ability to manage the issues.

5.3.2.1.3 Education Dimension

Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?

TCSE 2: In my case, there was no technical prerequisite or qualification for me, but I did have to pass certain exams before starting this job. In addition, on-the-job training is usually conducted by two means. The first way is that senior computer forensic investigators offer their experiences as teaching materials. The second way is by attending (inter)national conferences, visiting relevant (inter)national organizations, and attending overseas training programs. I have done this job for around one year.

Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?

TCSE 2: The current training methods for new staff have changed and improved. The training methods contain more dimensions, and are more formal. For example, certain computer forensic training courses are applied to train new staffs. These courses include legal knowledge and technical skills. My organization is trying to set up a standard training program.

Question 9: In your country, are there any tertiary-level courses that teach computer forensics?

TCSE 2: I think that CPU is the only university that teaches computer forensic courses. I do not think that usual universities contain computer forensic courses.

5.3.2.1.4 Law Dimension

Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?

B) In your own experience, what is the level of legal knowledge that computer forensic analysts have?

TCSE 2: A) I agree with the statement, and I think the understanding is necessary.

B) From my understanding, there is no such a law which precisely defines computer forensic issues although some laws contain relevant issues. In addition, I think that computer forensic analysts need to put more emphasis on legal issues. They normally are not familiar with legal issues. However, I have to admit that this is very hard to be achieved due to shortage of time, and lack of manpower. This situation should be improved by the cooperation between my organization and some legal departments.

Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?

B) In your own experience, what is the level of computer forensic knowledge that members of the court have?

TCSE 2: A) I agree with the statement. In addition, I believe computer forensic investigators and members of the court should spend more time and more efforts to understand each other's expertises.

B) From my personal experience, only limited number of members of the court understands computer forensic issues. Most of them are law experts rather than computer forensic experts. This situation should be improved by cooperation between my organization and some legal departments. However, the cooperation issue is beyond my ability.

5.3.2.1.5 Personal Preference and Skill Dimension

Question 12: As a computer forensic professional, do you use data wiping tools and/or data encryption tools for your data?

TCSE 2: Normally, I use both tools for personal data.

Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?

TCSE 2: Attending computer forensic courses, exams, and conferences are three major ways to upgrade the technical skills of computer forensic specialists. In addition, sending computer forensic investigators overseas for the advanced training programs is a well-accepted method.

5.3.2.2 Interpretations of the Second Case Study Findings

TCSE 2 provided his professional opinions based on his practical experience, and was able to explain his opinions freely. The aim of this case study is to discover the particular thoughts and opinions of TCSE 2. In this section, the researcher further interprets TCSE 2's opinions from a cultural perspective. Based on these cultural interpretations, insight into the specific behaviours of people in Taiwan on computer forensic issues can be drawn. Furthermore, these explanations are made based on the five dimensions in order to understand the computer forensic conditions thoroughly.

5.3.2.2.1 Current Situation Dimension

There are four questions in total in this dimension, and they are Question 1 to 4. These four questions are listed as follows.

- ***Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.***
- ***Question 2: Generally speaking, there are two common means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?***
- ***Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?***
- ***Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?***

In Question 1, TCSE 2 agreed that the importance of computer forensic SOPs, but also said that there is no such SOPs within his organization. This phenomenon is explainable by understanding the nature of Taiwanese culture. Taiwanese culture normally ignores the long-term objectives, and puts more attentions on short-term goals. As long as there is a solution for the current situation, the quality of this solution is not the primary

concern. In Taiwanese culture, unnecessary changing should be avoided. Changing or improving only takes place when there is an urgent need. The cultural understanding of this question is confirmed by Hofstede's research results (1980). Hofstede agreed that uncertainty avoidance is part of Taiwanese culture. This means that the finding of this question is trustworthy as it can be independently confirmed with Hofstede's work.

TCSE 2 agreed that he encountered two situations mentioned in Question 2. Nevertheless, he stated that it is a better choice for him to do the seizure, since there are usually errors discovered when the digital evidence is processed by other people and/or organizations. This situation can be explained by the nature of Taiwanese culture. Focusing on short-term objectives is part of Taiwanese culture. Hofstede (1980) proposed a similar concept for this situation, and used the term, '*uncertainty avoidance*', to describe this situation. Here, this thesis needs to clarify a standpoint. This research is not suggesting that every police officer needs to learn advanced computer forensic skills, but they at least have to have basic understanding about computer forensic issues. For example, the understanding may include what they can do and what they cannot do. Unfortunately, the finding of this question demonstrates that most of police officers do not have enough understanding of computer forensics.

In Question 3, TCSE 2 stated that he does not think staffing levels are high enough to deal with the computer forensic needs of the jurisdictional scope. The findings of this question points out that there are some values within the field of computer forensics beyond the influence of culture. In addition, the findings also respond to the outcomes of Delphi Question 30. In reality, Taiwanese government cannot provide unlimited financial support for the development of computer forensics. There are always other issues that need to be considered. In conclusion, the shortage of computer forensic workers is caused by monetary problems, and is not affected by the culture.

In Question 4, TCSE 2 stated that there are two distinct ways to recruit new computer forensic employees. The first way is using exams to evaluate the ability of future employees, and this is the major method for the recruitment. In addition, the second way of recruiting new staffs is to transfer the employees of other departments (e.g. computer security department) to computer forensic department. Since the second recruiting method is not affected by culture, the cultural interpretation can only be provided for the first recruiting method. Using exams to decide the ability of an individual is very

common in Taiwanese culture (Haifeng 2006). It is believed that the professional knowledge of an individual can be revealed by exams. In summary, using examinations is a well-accepted method for recruiting new employees in Taiwan.

5.3.2.2.2 Policy and Organization Dimension

There are two questions, Question 5 and 6 of the case study questionnaire, that discuss policy and organization within the field of computer forensics. These two questions are listed as follows.

- ***Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.***
- ***Question 6: In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.***

TCSE 2 confirmed the answer of Question 5 is affirmative. The development of computer forensics is beyond the development of current policies and legislation. Possible disputes for digital evidence can be prevented by well-defined policies and legislation. In reality, there are many challenges to improve the current development of computer forensic policies and legislation. An interesting viewpoint was found based on the opinion provided by TCSE 2. He stated that the purpose of his work is only to ensure the quality of the digital evidence, and he cannot help to change the current condition of computer forensic policies and legislation. The findings of this question can be explained by the nature of Taiwanese culture from three different perspectives. The first cultural perspective describes that short-term objectives obtain more attentions in Taiwanese culture. Thus, it is reasonable that the development of laws cannot keep up with the development of computer forensics, since there is no urgent need for new legislation. In addition, the second cultural perspective indicates that the government policies of computer forensics indeed affect developments of computer forensics. This is because collectivism is more popular than individualism in Taiwanese culture. This infers that an individual is essentially seeking to be identified with his or her group. Therefore, the behaviours and attitudes of an individual are more easily affected by outside factors and variables. An individual tends to agree with the conclusion

developed by others, and to follow the decision made by others as well. Lastly, the third cultural perspective shows an interesting and typical attitude of Taiwanese culture. TCSE 2 stated that he can do nothing to change the computer forensic policies and legislation. This is because that people in Taiwan normally worry about their own issues, and do not care about other issues. These three cultural explanations are confirmed by the discoveries of Hofstede's work (1980). According to Hofstede, uncertainty avoidance and collectivism are two attributes within Taiwanese culture. In summary, the above cultural standpoints explain the answers of TCSE 2 for Question 5, and these cultural perspectives are reliable.

In Question 6, TCSE 2 stated that MJIB and CIB are two central (federal-level) government organizations, which can deal with computer forensic issues. This infers that there is no local (state-level) computer forensic laboratory in Taiwan. In addition, TCSE 2 is not familiar with the situation outside the police system. This reaffirms that avoiding uncertainty is part of Taiwanese culture. This standpoint is supported by Hofstede (1980) and is discussed in the previous question. Since there are federal-level organizations for computer forensic purposes, the establishments of state-level computer forensic organizations are not an urgent issue. This points out that the essence of the issue is sometimes overlooked by Taiwanese culture. After all, it is impossible for federal-level computer forensic organizations to satisfy the computer forensic needs for the entire country. In addition, there is a cultural reason why TCSE 2 is not familiar with the current situations outside the government organizations. People in Taiwan only care about their issues, and do not think of others' issues. This is because they try to avoid any possible uncertainty. Understanding another person's and/or another organization's issues is not the top priority in Taiwanese culture.

5.3.2.2.3 Education Dimension

There are three questions, Question 7, 8, and 9 of the case study questionnaire, in this dimension, and they are listed as follows.

- ***Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?***

- ***Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?***
- ***Question 9: In your country, are there any tertiary-level courses that teach computer forensics?***

The findings of Question 7 and 8 can be explained jointly by the nature of Taiwanese culture. TCSE 2 agreed that there is no requirement for him when he started his current job. However, he did pass some exams for this job. TCSE 2 further said that the major on-the-job training is learning from the senior computer forensic investigators, attending national or international conferences, and attending overseas training programs. In addition, TCSE 2 agreed that the current training methods for new employees are improving and changing. For example, the training program currently contains legal knowledge and technical skills. The above situations can be explained by Taiwanese culture from two perspectives. The first viewpoint describes that Taiwanese culture is likely to seek the only truth for a question. Hofstede (1980) pointed out the same result, and believed that this is a typical attitude in Taiwanese culture. Thus, it is not surprising that TCSE 2's organization is changing the way it trains its computer forensic investigators, and is looking for a standard training program. In addition, sending computer forensic investigators overseas for advanced training shows that science is not a topical issue in Taiwan. Due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b), Taiwanese culture does not place attention on the value of science (Western scientific values). In summary, the answers of Question 7 and 8 are actually affected by the uniqueness of Taiwanese culture.

In question 9, TCSE 2 believed that CPU is the only university which has computer forensic courses. In reality, Tamkang University (Tamkang University 2007) and National Kaohsiung First University of Science and Technology (National Kaohsiung First University of Science and Technology 2007) have relevant courses as well. This phenomenon shows that there should be more attentions paid to the current conditions within educational issues within the field of computer forensics. A cultural explanation can be provided for this phenomenon. People in Taiwan normally do not prepare for problems which are not yet occurring. They usually face problems when they actually encounter the problems. This type of cultural attitude is called uncertainty avoidance in

Hofstede's research (1980). According to Hofstede, Taiwanese culture has strong uncertainty avoidance. This infers that the cultural explanation for this question is reliable.

5.3.2.2.4 Law Dimension

There are two questions in this dimension, and they are Question 10 and 11 of the case study questionnaire. These are listed as follows.

- ***Question 10: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for a computer forensic investigator to understand law relevant issues'?***

  B) In your own experience, what is the level of legal knowledge that forensic analysts have?
- ***Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?***

  B) In your own experience, what is the level of legal knowledge that members of the court have?

The findings of Question 10 and 11 can be explained jointly by the nature of Taiwanese culture. According to TCSE 2, the understandings between computer forensic investigators and members of the court are not enough, and this situation should be improved and changed. In addition, TCSE 2 also stated that improving this situation is beyond his ability. The discoveries of these two questions can be explained by the nature of Taiwanese culture. People in Taiwan typically concern their problems first, and believe that '*if I cannot solve my own problem, how could I help to solve other people's problems?*'. This situation shows that people in Taiwan are only responsible for their own work, and try to avoid any possible uncertainty. In addition, Hofstede (1980) called this situation uncertainty avoidance, and Taiwanese culture is considered strong uncertainty avoidance. Thus, the findings of Question 10 and 11 are not reasonable.

5.3.2.2.5 Personal Preference and Skill Dimension

There are two questions in this dimension, and they are Question 12 and 13 of the case study questionnaire. These two questions are listed as follows.

- ***Question 12: As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?***
- ***Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?***

In Question 12, TCSE 2 stated that he normally uses both data encryption and wiping tools. This is explainable from a cultural perspective. In Taiwan, competitions in every aspect of society for better results are very common and often acrimonious. This is mainly because there is a larger population than available resources. This argument is proved by Hofstede (1980) and is discussed in Taiwanese Delphi Question 28. In short, it is reasonable for the uses of data wiping tools and/or data encryption tools, since it is a helpful way to protect one's privacy and property.

In Question 13, TCSE 2 stated that attending computer forensic courses, exams, and conferences are three major ways to upgrade the technical skills of computer forensic specialists. In addition, sending computer forensic investigators overseas is another popular choice as well. The finding of Question 13 can be explained by understanding the nature of Taiwanese culture. The value of science (Western scientific values) is not respected by Taiwanese culture due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). Thus, Taiwanese culture is used to follow the lead of Western science. This inference is discussed in the Delphi Question 1, 2, and 3. In summary, it is understandable that computer forensic investigators are usually sent overseas for advanced training and educational purposes.

5.3.2.2.6 Cross Questions

In this section, the researcher tries to further establish the possible relationship between case study questions. This section builds the relationship between Question 7 and 8. The findings of Question 7 cannot directly corroborate the results of Question 8, but combining the outcomes of these two questions shows that the computer forensic

training are changing and improving in TCSE 2's organization. In Question 7, TCSE 2 stated that he had to pass several exams for his current job. In addition, TCSE 2 stated, in Question 8, that the present training programs are more systematic. In summary, combining the answers of these two questions points out that the situations for computer forensic training in TCSE 2's organization are improving and changing.

5.3.3 Comparison of Taiwanese Case Studies

In general, two Taiwanese case studies show very similar discoveries. It is actually found that TCSE 1 and TCSE 2 have very close opinions on the case study questions. In addition, this section uses other types of data to demonstrate the trustworthiness of the opinions from two case study participants. This situation is appropriate since the concept of case study allows the use of various data sources. The detailed discussions of case study can be found in the Section 3.6. Nevertheless, one viewpoint should be clearly explained before the following paragraphs. The researcher cannot ensure that there are other types of data sources for every case study question. The multiple data sources of some questions may not be found.

In Question 1, TCSE 1 and TCSE 2 both admitted that the importance of computer forensic SOPs. This argument is supported by Lin *et al* (2003a) and Lin *et al* (2003b), which were proposed by Taiwanese academic researchers. These two papers also emphasize the significance of the issues associated with the computer forensic SOPs. The existence of these two papers demonstrates the trustworthiness of the opinions provided by TCSE 1 and TCSE 2.

In Question 6, TCSE 1 and TCSE 2 both stated that MJIB and CIB are two government organizations, which are able to deal with computer forensic issues. This statement is correct by referring the following data. Reports (Radio Taiwan International 2006; IThome online 2006) support the descriptions provided by TCSE 1 and TCSE 2. MJIB established computer forensics laboratory on 26/12/2006. At the beginning, there were only four agents working in the cyber forensics laboratory. The situation was improved when the researcher visited the cyber forensics laboratory on 03/07/2007. There are six agents at this moment. The future plan is going to have eight agents in order to deal with the increasing number of computer crimes.

In Question 9, TCSE 1 and TCSE 2 both stated that there are computer forensic courses taught in CPU. This situation is reasonable, since CPU is directly managed by Ministry

of the Interior. Due to the unique role of CPU, several peculiar departments, which can rarely be seen in other universities, can be found in Central Police University. For example, these departments are: Department of Border Police (Department of Border Police 2007), Department of Maritime Police (Department of Maritime Police 2007), Department of Fire Science (Department of Fire Science 2007), Department of Public Security (Department of Public Security 2007), and Department of Forensic Science (Department of Forensic Science 2007).

According to the uniqueness of previous departments, it is not surprising that Department of Information Management of CPU (Department of Information Management 2007) not only has basic computer courses, but also contains computer forensics courses. In addition, Tamkang University (Tamkang University 2007) and National Kaohsiung First University of Science and Technology (National Kaohsiung First University of Science and Technology 2007) are two other universities which also teach computer forensic courses. Moreover, Taiwan Computer Emergency Response Team/ Coordination Centre (TWCERT/CC) (Taiwan Computer Emergency Response Team/Coordination Centre 2007) is another organization that provides relevant services and courses for computer forensics. The services include education and training of computer forensic experts.

5.3.4 Summary of Section 5.3

Two Taiwanese Case Studies are introduced in Section 5.3. Section 5.3.1 introduces the first Taiwanese case study, and examines three quality factors of this case study. These factors include quality of the first case study organization, quality of case study participant, and quality of case questionnaire. This means that the quality of the first case study findings, which are discussed in Section 5.3.1.1, are ensured and proved. Lastly, the cultural interpretations for these findings are listed in Section 5.3.1.2.

Section 5.3.2 examines the same quality factors for the second Taiwanese case study. The quality of the two Taiwanese case study interviews is the most concern in this thesis. The quality of the results of two case studies can only be ensured with high quality preparations. In addition, Section 5.3.3 uses additional information to support the certain opinions provided by TCSE 1 and TCSE 2. In summary, Section 5.3 not only

introduces the two Taiwanese case studies, but also confirms the relationship between these two case studies.

5.4 Triangulation and Corroboration of Research Results

5.4.1 Triangulation of Research Methods

Historical data, Delphi survey, and case study interview are three different methods used in this thesis in order to achieve methodological triangulation. The use of methodological triangulation is able to prove the trustworthiness of the major research question in this research. The concept of triangulation is discussed in the Section 3.4.5. In this section, Figure 11 shows the relationship among the three different research methods. In addition, two case study interviews are actually providing very similar and close results. This means that these two case studies can be considered a whole, and can be discussed together for the further triangulation issues.

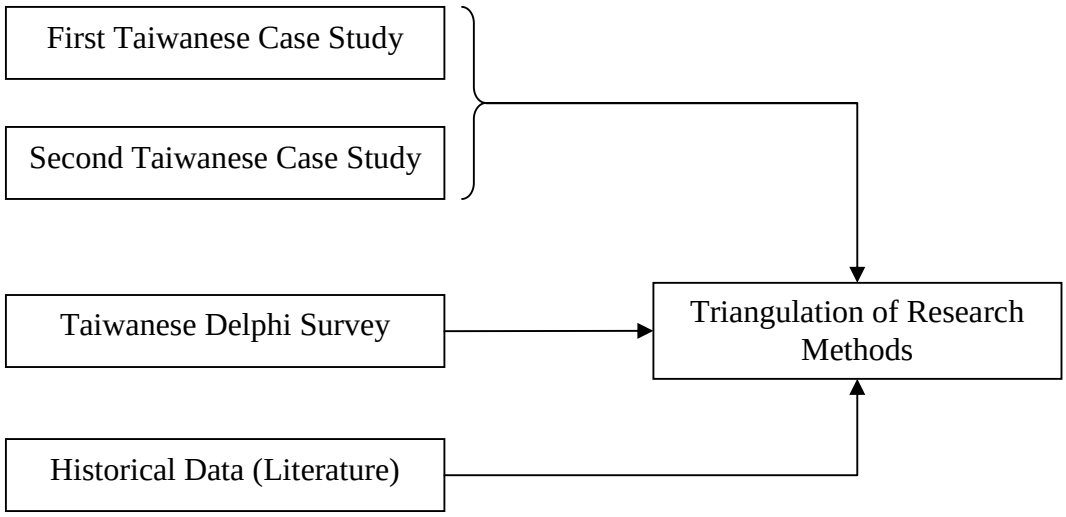


Figure 11: The Triangulation of Research Methods in Taiwan

The historical data, literature, not only introduces the basic understanding of computer forensics, but also proves that computer forensics is a subject within the field of science in Section 2.2. In addition, Section 2.3 shows that the meaning of culture, and culture is able to affect applications of science. Therefore, combining the discoveries of Section 2.2 and Section 2.3 is able to lead to a reasonable inference, which describes computer forensic applications are affected by different cultures.

In addition, the interpretations of Delphi results proposed in Section 5.2.3 confirm the relationship between Taiwanese behaviour on computer forensic issues and Taiwanese culture. Although 10 out of 40 questions are not affected by Taiwanese cultures, there are reasonable cultural explanations for the other 30 questions. In short, the discoveries of Delphi survey are able to prove that culture is one of the factors to affect computer forensic applications.

Lastly, the interpretations of two Taiwanese case study interviews in Section 5.3.1.2 and 5.3.2.2 demonstrate the existence of the relationship between computer forensics and Taiwanese culture as well. Although Question 3 (for both case study interviews) is beyond the influence of culture, rational cultural explanations can be provided for the other 12 questions (for both case study interviews). In summary, the discoveries of case study are able to prove that certain computer forensic applications are affected by Taiwanese culture.

In conclusion, the results of these three methods are able to corroborate the relationship between Taiwanese culture and computer forensics. This means the methodological triangulation is achieved, and the trustworthiness of the results from three research methods is improved and more convincing.

5.4.2 Corroboration for Delphi Survey and Case Study

After Taiwanese Delphi survey and case study interviews, it is realized that the findings of some Delphi questions actually match the results of case study questions, and vice versa. This indicates that the trustworthiness of certain Delphi results are proved and enhanced by findings of case study questions, and vice versa. In here, two Taiwanese case studies are considered as a whole, since they have close findings. Thus, in this section, the term '*case study*' actually represents the first Taiwanese case study and the second Taiwanese case study.

Corroborations for the interpretations of Delphi results and case study findings are provided for the further verification of the relationship between computer forensics and Taiwanese culture. The relationships between Delphi questions and case study questions can be found in the Table 19.

Table 19: Relationships between Case Study Questions and Delphi questions

Case Study Question 1	Delphi Question 5
Case Study Question 3	Delphi Question 30
Case Study Question 4	Delphi Question 17
Case Study Question 5	Delphi Question 38
Case Study Question 6	Delphi Question 13
Case Study Question 7 and 8	Delphi Question 17 and 22
Case Study Question 11	Delphi Question 30, 35, and 36
Case Study Question 12	Delphi Question 39 and 40
Case Study Question 13	Delphi Question 22 and 32

The Delphi questions mentioned in the Table 19 are listed as follows.

- ***Question 5: From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?***
  - ***Derivative Question (Question 2 in the Round Two Delphi Questionnaire): Due to different organizations and/or different understandings, there is more than one guideline for computer forensics. Unfortunately, there is no specific SOPS for computer forensic purpose at this moment. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 13: In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?***
- ***Question 17: How are computer forensic experts produced in your country? through what kind of tests? or procedures?***
- ***Question 22: In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?***
- ***Question 30: Based on your knowledge, have performing computer forensic investigations in your country suffered any difficulty? Can you briefly list them?***
- ***Question 32: Based on your knowledge, have computer forensic organizations/departments/agencies in your country ever had interactions with international organizations/departments/agencies related to similar***

area? If "YES", how do they interact with other organizations/departments/agencies in other countries?

- ***Question 35: In your experience, do courts give a high or low weighting to digital evidence in your country?***
    - ***Derivative Question (Question 11 in the Round Two Delphi Questionnaire): In Taiwan, although the court cannot overlook the importance of digital evidence, the court normally gives a low weighting to digital evidence. The only exception is that the digital evidence is valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions?***
- ***Question 36: Do you know of any difficulties caused by using digital evidence in court? If "SO", what has been the major reason for this?***
- ***Question 38: Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If "SO", does this affect the attitude of computer forensic investigators to perform investigations? If "YES", can you briefly explain?***
- ***Question 39: As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?***
- ***Question 40: As a computer forensic professional, do you use any type of encryption tools for the data in your work?***

In addition, the case study questions mentioned in the Table 19 are listed as follows.

- ***Question 1: In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.***
- ***Question 3: Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?***
- ***Question 4: In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?***

- ***Question 5: Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.***
- ***Question 6: In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.***
- ***Question 7: Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?***
- ***Question 8: What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?***
- ***Question 11: A) Do you agree with and what is your opinion of the following statement: 'It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics'?***

  B) In your own experience, what is the level of legal knowledge that members of the court have?
- ***Question 12: As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?***
- ***Question 13: How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?***

In the following paragraphs, discussions on the relationships between the Delphi questions and case study questions are introduced. The findings of Question 1 of case study questionnaire match the results of Question 5 of the Round One Delphi questionnaire. The outcomes of these two questions not only show that there is currently no computer forensic SOPs in Taiwan, but also improve the trustworthiness of these outcomes. In short, the issues of computer forensic SOPS are confirmed by two different research methods.

In Question 3 of case study questionnaire, two case study participants stated that the staffing levels are not enough for the current digital incidents. These findings match the

outcomes of Delphi Question 30. In Question 30, Delphi consensus shows that lack of computer forensic workers is one of the current problems. In summary, the findings of Question 3 of case study questionnaire corroborate the outcomes of Question 30 of the Round One Delphi questionnaire, and vice versa.

The findings of case study Question 4 and the discoveries of Delphi Question 17 are very similar. In this case, the quality of these discoveries can be enhanced by examining the similarities. In fact, Delphi Question 17 shows that there are multiple methods to train a computer forensic expert. Unexpectedly, the answer of Question 4 of case study questionnaire is one of these methods. This improves the trustworthiness of findings of the Delphi survey (Question 17) and the case study (Question 4).

The discoveries of case study Question 5 and the outcomes of Delphi Question 38 are very similar, and mainly claim that the imperfection of legislation does affect the attitudes of computer forensic investigators. This is because the collectivism is one of the major beliefs in Taiwanese culture (Hofstede 1980). They may work negligently if there is no clear rule or legislation. In summary, corroboration improves the trustworthiness of the findings of case study Question 5 and Delphi Question 38.

The discoveries of case study Question 6 and Delphi Question 13 agree that only central (federal-level) government organizations have the ability to deal with computer forensic issues, such as MJIB and CIB. This indicates the discoveries are confirmed by two distinct research methods, and the trustworthiness of these discoveries is enhanced.

The findings of case study questions (Question 7 and 8) point out that there is no standard training program for computer forensic investigators in Taiwan. These findings match the outcomes of Delphi questions (Question 17 and 22), which also show that there are multiple ways to train a computer forensic investigator. In summary, these four questions confirm that the there are multiple training methods for computer forensic investigators in Taiwan at this moment. The standard training method is an ongoing project.

The findings of case study Question 11 corroborate the results of Delphi Question 30, 35, and 36. According to the findings of case study Question 11, it is not surprising that Delphi consensus shows that the low weighting is given to digital evidence (in Delphi

Question 35), and members of the court have poor understanding of computer forensic issues (in Delphi Question 30 and 36). After building the relationship between case study Question 11 and three Delphi questions (Question 30, 35, and 36), the findings of previous four questions are considered more reliable.

The findings of case study Question 12 match the results of Delphi Question 39 and 40. The answers of TCSE 1 and TCSE 2 corroborate the Delphi consensuses which are provided by ten Taiwanese Delphi respondents, and vice versa. This infers that the outcomes of these three questions are proved to be more reliable.

The findings of case study Question 13 match the results of Delphi Question 22 and 32. In this case, the answers of case study Question 13 prove the results of Delphi Question 22 and 32. Combining the findings of these three questions confirms that there are training methods in Taiwan, and the existence of interactions between Taiwanese and foreign computer forensic organizations. In conclusion, the corroborations for case study Question 13 and two Delphi questions (Question 22 and Question 32) prove the trustworthiness of these findings.

5.4.3 Summary of Section 5.4

In Section 5.4.1, combining the inference of historical data, cultural interpretations of Taiwanese Delphi results, and cultural interpretations of Taiwanese case study findings points out that the concept of triangulation is achieved. The results of these three research methods confirm that culture is able to affect computer forensic applications, and respond to the research question of this thesis. In addition, Section 5.4.2 shows that the findings of some Delphi questions are actually confirmed and verified by the outcomes of certain case study questions, and vice versa. The corroborations prove the trustworthiness of these questions.

5.5 Summary of this Chapter

According to the Delphi survey and case study, the current conditions of computer forensics in Taiwan are revealed. According to the discoveries of these two research methods, there are some questions beyond the influences of culture. The questions without cultural explanation are Question 4, 6, 8, 9, 12, 24, 26, 29, 30, and 31 in the

Round One Delphi questionnaire, and the Question 3 of the case study questionnaire. The concepts of these 11 questions are related to global and independent values, which are not affected by different cultures.

On the other hand, there are reasonable cultural explanations for the rest questions in the Round One Delphi questionnaire and case study questionnaire. This indicates that particular Taiwanese behaviours within the field of computer forensics are explainable from cultural perspectives. To researcher's best understanding, this is the first research to discuss the computer forensics from cultural perspectives. In summary, the current circumstances of computer forensics within Taiwan are mainly caused by the following characteristics of Taiwanese culture.

- Taiwanese culture accepts Confucianism as major educational trend.
- Taiwanese culture does not emphasize the value of science (Western science).
- Taiwanese culture emphasizes the value of examination
- Taiwanese culture follows the lead of Western countries in the field of science.
- Taiwanese culture seeks for the unambiguous answer.
- Taiwanese culture focuses on short-term objectives.
- Taiwanese culture is not willing to take the challenges, and tries to avoid possible uncertainty in the future. '*What is different is dangerous*' is believed.
- Taiwanese culture seeks the identification within the group.
- Taiwanese culture believes there are different values between in-group and out-group.
- Taiwanese culture interprets the hierarchy as the nature of inequality.
- Taiwanese culture believes that the supervisor is inaccessible.
- Taiwanese culture is competitive.

6 Discussion on the Differences between Australian and Taiwanese Culture

6.1 Overview of this Chapter

This chapter compares and contrasts the Australian and Taiwanese cultural interpretations that have been independently discussed in Chapter 4 and 5, and provides an overall understanding of computer forensic issues occurred in Australia and Taiwan. The aim of this chapter is to compare the conclusions that have been developed for each culture independently, and to understand where and to what extent the similarities and differences are. To do this, each dimension of the Delphi survey and case study interviews will be discussed regarding similarities and disparities. A greater understanding of the underlying reasons for particular areas may be explained with reference to the case study interviews.

6.2 Current Situation Dimension

This section discusses the Delphi questions and case study interviews related to the current situation of computer forensics. These have already been discussed independently in sections 4.2.3.1, 4.3.1.2.1, and 4.3.2.2.1 for the Taiwanese experts (Delphi survey instrument and experts respectively), and sections 5.2.3.1, 5.3.1.2.1, and 5.3.2.2.1 for the Australian experts (also Delphi survey instrument and experts respectively). Within this dimension there are a number of different comparisons that may be drawn.

Questions 1, 2, and 3 within the Delphi survey instruments provide an overall understanding of the current situation within the field of computer forensics. Within the field of computer forensics, it is reasonable, as part of Western society, to have similar cultural background and close relationship with the United States of America (Albinski 2001; McLean 2006) and Great Britain (Horne 1964; Goldsworthy 2005), who are both very strong in the development of computer forensics from both a practitioner perspective and in the area of research. This interpretation can be based on the findings of the Delphi Questions 1, 2, and 3 from the Australian surveys, as outlined in Chapter 4. These questions imply a strong correlation between scientific principles and Australian computer forensic methods and underpinnings. In addition, Australia's close heritage and close political ties with the United States of America and the United Kingdom allows for an exchange of ideas and technology.

On the contrary, the value of science (Western scientific values) is comparatively lower in Taiwan, and this may be due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). Taiwanese culture has traditionally followed the lead of Western countries within the field of science, rather than being at the forefront. The value of science is not highly respected in Taiwanese culture. With this understanding, the results of Delphi Question 1, 2, and 3, provided by Taiwanese respondents in Chapter 5, may be better understood. These responses do reflect this cultural attitude (for more information, please see Chapter 5).

In summary, the differences between Australian and Taiwanese culture are able to explain the findings of Delphi Question 1, 2, and 3. However, these outcomes also show the vast differences in the cultures as they reflect on the field of science, and how this affects the field of computer forensics. These are the differences outlined in the first three questions of the common Delphi survey.

Delphi Question 5 and 7, and case study Question 1 discuss common themes and as such can be discussed jointly. Australian culture emphasizes the value of science, and this is reflected in research. An Australian scientific world view was provided by Slay (2000b). Therefore Australian culture normally focuses on a specific issue and attempts to find a corresponding scientific solution. Thus, the existence of computer forensic SOPs and relevant legislation are predictable and reasonable responses in Australia, being the outcome of implementation-based research. On the contrary, Taiwanese culture tends to focus on the uncertainty avoidance. This standpoint is supported by Hofstede (1980). This indicates that the development of computer forensic SOPs and relevant legislation does not have highest priority unless there is an urgent need for them. In short, Australian and Taiwanese cultures provide different answers to the same issue. The answers to these two Delphi survey questions and case study interview question confirms this, and show a vastly different pattern in research and the state of development of SOPs.

Question 10 of the Delphi survey instrument seeks opinion and feedback on the attitudes toward the trustworthiness of meta-data of digital evidence. The outcomes of this, as described in Chapter 4 and Chapter 5, indicate that there are differences in the trustworthiness of meta-data between Australia and Taiwan. In Australia, Delphi experts actually consider meta-data of digital evidence another type of digital evidence.

Thus, they accept the trustworthiness of meta-data of digital evidence as long as digital evidence is proved reliable. There are potentially two factors for this; Australia taking some legal precedent from the United Kingdom and their common law approach (Cater 1995; Heilbronn *et al* 2002), indicating that culturally, Australia does take some input from the Commonwealth and Britain in particular. It also shows that people in Australia have less trouble in accepting new concepts or novel technologies. This shows the tolerant nature of Australian culture (Hofstede 1980). On the other hand, Taiwanese Delphi experts expressed that the trustworthiness of meta-data of digital evidence is believed due to the reliability and validity of computer forensic tools. If the computer forensic tool is sound, its products, including meta-data of digital evidence, are firm and solid as well. This demonstrates that Taiwanese culture puts more focus on the unambiguous answer (Hofstede 1980). In short, the findings of Question 10 show that the trustworthiness of meta-data of digital evidence is considered from different perspectives in Australia and Taiwan. This outcome is potentially important to any cooperation between the two countries, or where these cultures intersect, and will be discussed further in the conclusion.

Question 11 of the Delphi instrument survey gauges the attitudes towards the relationship between the fields of computer security and computer forensics. The outcome of these questions, as independently discussed for Taiwan in Chapter 4 and Australia in Chapter 5, is that Australia and Taiwan have completely different attitudes toward the relationship between computer security and computer forensics. In Australia, Computer security and computer forensics are considered two entirely different fields of study. This is possibly because Australian culture emphasizes independence and autonomy (Hofstede 1980). Computer security is proactive to protect digital incidents from occurring, whereas computer forensics is reactive to respond the occurred digital incidents. This concept has also been supported by the Taiwanese experts in both the Delphi instrument and the interview. Nevertheless, the difference between the two country's outcomes is that Taiwanese experts believe in a much closer relationship between computer security and computer forensics work, and that they cooperate and interact as a cycle. Computer security is the front end of this cycle, and computer forensics is the back end of this cycle. Well-developed computer security provides a better opportunity for computer forensics to collect relevant digital evidence. In addition, the capability of computer forensics can enhance the level of computer

security. This is potentially because Taiwanese culture emphasizes interdependence (Hofstede 1980).

In summary, the attitudes of the relationship between computer security and computer forensics are considered differently in Australia and Taiwan. Whereas the Taiwanese experts surveyed and interviewed saw a common and strong link between computer security and computer forensics, the Australian experts see much less of a commonality between the two areas.

Question 27 of the Delphi survey instrument given to both Australian and Taiwanese experts asked about the importance of time issues in computer forensic investigations. The outcome of this question was common to both Australian and Taiwanese experts, with both expert groups affirming its importance. The outcomes of the Australian Delphi survey and the case study interviews introduced two time-related issues, and these were introduced in Chapter 5 of this work. Specifically, Australia has multiple time zones within the country and also has daylight saving time over the summer months. For these reasons, Australian computer forensic investigators specifically spend more effort ensuring correct times when they collect the digital evidence. Whilst this is an issue within Australia, it is not in Taiwan, which neither has multiple time zones or any form of daylight saving time. According to the findings from Chapter 4 by Taiwanese Delphi experts, time related issues are the first concern when computer forensic investigators receive any form of digital evidence.

In summary, although time issues are recognized important in both Australia and Taiwan, two cultures treat time issues from different perspectives. From a perspective of interoperability between the two cultures, there are some interesting differences that must be accounted for. For instance, if digital evidence originating from Australia is examined in Taiwan, the analyst would need to confirm the time whilst remembering both the time zone from which that evidence was recovered and the state of daylight saving for both that state and date. However, given that both countries place a strong emphasis on any element relating time and date with electronic evidence then this does not prove a major hurdle for cross-cultural cooperation.

In the Delphi survey instruments, question 28 seeks to understand the percentage of encrypted data that computer forensic investigators encounter. The outcome of this indicates that encrypted data makes up between 0% and 20% of investigations in both

Australia and Taiwan. There are a number of reasons for this response; some cultural, and some not. The non-cultural reason for such a low percentage of encrypted data in analysis is that applications that allow seamless encryption are only now becoming standard, and also that the overhead of encryption is relatively high. Therefore many individuals have not had the technical skills or equipment to correctly implement encryption until recently. From a cultural perspective, the findings are also reasonable since the Australian living style is considered relaxed and comfortable (Horne 1964). Australian culture does not emphasize the concept of competition, and does not place major attention on prevention and protection. In Taiwan, the same result can be explained from another cultural perspective. People in Taiwan are normally keen to protect their property due to extreme competition, anxiety, and stress (Hofstede 1980). Nevertheless, the Taiwanese Delphi results do not show this cultural difference. The possible answer for such a low use of encryption in digital evidence and no obvious cultural explanation is that criminals in Taiwan do not completely understand computer technologies. In summary, the findings of Delphi Question 28 show that in both Australia and Taiwan, there is a low use of encryption found in investigations. Whilst there are many explanations for this, there are certainly cultural influences that impact these numbers.

In case study Question 2, Australian case study interviews reveal different results from Taiwanese case study interviews. In Australia, two case study participants stated that there is no explicit difference between the two collection methods mentioned in this question. As long as a non-technical individual does not process the seized data, there is no serious problem for these two collecting methods. This is because Australian culture is able to accept legitimate dissent (Hofstede 1980). A particular method is unacceptable only if it breaks the laws and/or jeopardizes its original purpose. On the contrary, Taiwanese case study participants stated that they prefer to seize the digital data themselves since errors are usually discovered. There is a reasonable cultural explanation for this phenomenon. Taiwanese culture tends to focus on short-term objectives. This concept is supported by Hofstede (1980) as well. The only difference is that Hofstede used the term, '*uncertainty avoidance*', to describe this concept. At present, computer forensics is only an interesting topic for particular groups (e.g. academic researchers and MJIB). This means the majority of police officers do not have enough understanding of computer forensic issues. In this case, the findings of this

question are not surprising. In summary, the issues of seized digital evidence encounter different problems in Australia and Taiwan.

Question 4 of the case study interviews discovered that there are differences in both the recruitment methods and skills that are needed for new staff in Australia and Taiwan. In Australia, advertising is a common way to recruit new employees. In addition, both Australian case study participants agreed that the ability and skills of an individual are more important than his or her educational qualifications. The cultural reason for this is that expertise and professional experience are respected in Australian culture (Hofstede 1980). However, TCSE 1 and TCSE 2 agreed that attending exams is the popular way when recruiting new employees in Taiwan. This situation is deeply affected by the concept of imperial examination (Haifeng 2006). Taiwanese culture suggests that a well-rounded education is required, and that examination is a means of determining a person's knowledge and skill. In short, Australian and Taiwanese culture adopts different methods to evaluate the ability of an individual and this may be reflected in their choice of forensic analysts.

6.3 Policy and Organization Dimension

This section discusses the Delphi questions and case study interviews related to policy and organization within the field of computer forensics for each culture. Again, each of the results from both the surveys and case study interviews have already been discussed separately and specifically to the culture, and this section aims to provide the comparison between cultures.

Delphi Question 13 and case study Question 6 for both cultures asks the respondents to provide information that helps determine the structure of organization within their workplace. In Australia, computer forensic organizations exist in federal-level and state-level law enforcement headquarters. This is necessary since Australia is a geographically large country. Hierarchical design is essential for convenient management. Similarly, whilst there are federal agencies, state policing agencies also maintain their own forensic capacity, and this is borne out of existing police structures. The answers to these questions also infer that computer forensics as a field is important, and that there is a need to perform computer forensic analysis at different policing agencies. In addition, private companies (e.g. accounting companies) also have the

ability to deal with computer forensic issues. The responsibilities of law enforcement agencies and private companies are clearly defined. This is understandable since Australian culture respects the classification of jurisdiction (Hofstede 1980). Federal-level law enforcement has different responsibility from state-level law enforcement. Furthermore, private companies have different duties from law enforcement agencies.

Taiwan, on the contrary, maintains only federal-level capacity in computer forensic analysis. This is mainly because that the government does not put enough resources into the development of computer forensics. Essentially, the staffing levels in central (federal-level) computer forensic organizations are not sufficient for the entire country. This situation shows that Taiwanese culture tends to avoid possible uncertainties (Hofstede 1980). As long as the solution exists, the quality of the solution is not the first concern. In addition, according to TCSE 1 and TCSE 2, it is further realized that the relationship between private companies and law enforcement agencies is not good. This phenomenon reflects that people in Taiwan usually consider their own problems first, and ignore other personally irrelevant issues. In short, the different cultural attitudes and existing policing infrastructures in Australia and Taiwan affect the development of computer forensics in these two countries. From an interoperability perspective, the two cultures have different structures in place for policing, and it may be an issue for a person in one country to find an equivalent technical analyst from another country. Also, it would be difficult to understand the relative ranks and processes between countries, given the complete disparity between the two.

Question 14 of the Delphi survey instruments given to both countries attempted to determine if either Australian or Taiwanese law enforcement outsource any of their forensic analysis to third parties. The outcome of this question showed that neither Australian nor Taiwanese law enforcement agencies outsource the analysis of digital evidence. In Australia, the classification of jurisdiction is explicit and respected. This standpoint is supported by Hofstede (1980). The only authorized organizations for criminal cases are law enforcement agencies. No private company has the right to analyse evidence for criminal cases. Since digital evidence has the potential to be presented in a court, it is understandable that law enforcement agencies should be the only organizations that can process digital evidence. On the other hand, the values and beliefs between the in-group and out-group are different in Taiwanese culture (Hofstede 1980). It is a strongly-held belief that a neutral organization can rarely be found in

Taiwan. This means the results, which are produced by the people in out-group, are sometimes hard to be believed by the people in in-group. Thus, it is reasonable for law enforcement agencies to deal with the digital data involved in criminal cases. After all, there is the potential that digital evidence potentially has a court –of-law outcome. In summary, cultural explanations can be found for this question to explain the different findings discovered by the Australian and Taiwanese Delphi surveys.

Question 15 of the Delphi surveys asked respondents to rate the effectiveness of the computer forensic readiness within their organizations. The outcome of this was that Australian Delphi consensus agreed that there is no computer forensic readiness within their organizations. This is logical since Australian culture is considered relaxed and casual (Horne 1964). Thus, Australian culture usually does not automatically focus on prevention and protection. Since there is no serious and immediate threat for computer forensic issues, there is no urgent need for computer forensic readiness and hence organizations may be under-prepared. In Taiwan, Delphi respondents agreed that most Taiwanese organizations, especially non-critical organizations, are not prepared for future forensic examinations. The cultural explanation for this is that Taiwanese culture focuses on the short-term issues, and seeks immediate results and conclusions (Hofstede 1980). Thus, it is understandable that there are rarely preparations for possible future trouble. In summary, the Australian and Taiwanese Delphi surveys revealed the same finding, but this finding is the result of different cultural underpinnings.

In the Delphi surveys, Question 16 sought to determine who was responsible for computer forensics, and if the same group was also responsible for other forms of computer security. In Australia, it was found that there are two different types of organizations who deal with computer security issues and computer forensic issues, and these two types of organizations have different capabilities and purposes. This is because Australian culture respects jurisdiction and responsibility. This perspective is also supported by Hofstede's research results (1980). Thus, it is reasonable that the Australian culture considers computer security and computer forensics two separated topics, and these two subjects are processed by two different types of organizations. This has also been discussed within the previous dimension. In addition, the results of the Taiwanese Delphi survey showed the same result. However, the Taiwanese underpinnings are believed to be caused by different cultural underpinnings. Since it has been established that scientific development in Taiwan is not culturally as important, the

Taiwanese government is learning computer forensics techniques and training from other countries (e.g. the United States of America). This argument is explained by the results of Delphi Question 16 in Section 5.2.3.2. In this case, the Taiwanese government realizes that computer security and computer forensics are two similar but different topics, and treats them differently as other Western countries. In summary, Australian and Taiwanese Delphi survey show the same finding, but this finding is the result of different cultural attitudes.

The findings of Delphi Question 32 and 33, discussed jointly, provide an overall understanding of the situation of computer forensic policies and organizations within the two countries. In Australia, electronic crime sections exist within the federal-level and state-level police headquarters (e.g. AFP and the SAPOL), and their responsibilities are defined very clearly. For example, the AFP organizes interactions with other international computer forensic organizations, and the SAPOL focuses on criminal cases within South Australia. However, regarding communications with universities and academia, this can occur at all levels and there are a number of state policing agencies with good relationships with Australian universities. This phenomenon can be explained by the different acknowledgements of jurisdictions and responsibilities, and can also be found in Hofstede's arguments (1980). Australian culture respects the fact that different organizations should have different responsibilities, and for policing, this is divided into jurisdictions. However, interacting with international computer forensic organizations provides a good opportunity to improve the current development of computer forensics in Taiwan. This method is a good way to gain valuable experience. When people in Taiwan are seeking for the latest knowledge within the field of science, they normally look for overseas resources as internal scientific development does not receive a large degree of attention (Jingpan 1990; Ho 1991). In addition, Taiwanese culture emphasizes the importance of interpersonal relationships. This standpoint is confirmed by Hofstede (1980) as well. Thus, the interactions within Taiwan are reasonable since the number of computer forensic workers and researchers are limited. A good interpersonal relationship is important in this small group. In short, the same findings were discovered in Australian and Taiwanese Delphi survey, but these findings are caused by different cultural attitudes.

In Delphi Question 34, Australian and Taiwanese respondents considered supervisors from different perspectives. Australian Delphi experts stated that they have interactions

with colleagues and supervisors. This is because people in Australian believe that supervisors are accessible, and that hierarchy is designed for easy management (Hofstede 1980). On the other hand, Taiwanese Delphi respondents expressed the belief that the interactions are mainly occurring between colleagues because people in Taiwan believe that supervisors are inaccessible. There is usually a gap between the supervisor and the corresponding colleague (Hofstede, 1980). In summary, different cultural perspectives yield different results for the same situation.

In case study Question 5, Australian case study participants (ACSE 1 and ACSE 2) both agreed that the government policies and their work are two independent things. This is caused by the nature of Australian culture, which concentrates on individualism and independence. According to Hofstede (1980), he also confirmed that the importance of individualism and independence within Australian culture. This means people in Australia are confident of their beliefs, standpoints and behaviours. On the contrary, TCSE 1 and TCSE 2 stated that the government policies on computer forensics indeed affect the development of computer forensics. The reason for this situation is that people in Taiwan tend to seek clear regulations and guidance. If the government policies on computer forensics are well-designed, possible disputes can be ruled out. Uncertainty is not a well-accepted concept in Taiwanese culture. This concept is supported by Hofstede (1980) as well. In addition, both Taiwanese case study participants stated that they are not in the correct position to change current computer forensic policies. This type of work is beyond their ability. In short, Australian and Taiwanese culture reflect that different cultures indeed have impacts on computer forensic applications.

6.4 Education Dimension

This section discusses the Delphi questions and case study interviews related to how each culture understands and relates education to the field of computer forensics. As with the previous sections of this work, each of the results from both the surveys and case study interviews have already been discussed separately and specifically to the individual culture, and this section aims to provide the comparison between the two cultures.

The results of Delphi Question 17, 18, 19, 21, and 22, and case study Question 7 and 8 can be discussed jointly to provide an overall understanding of the educational situation within the field of computer forensics. In Australia, there is no standard way to produce a computer forensic expert, and there is also no organization that definitively is able to certify the qualifications of computer forensics experts. In addition, there are multiple ways to train computer forensic investigators in Australia, and on-the-job training is the major method for the training of computer forensic investigators. The situation discovered in Australia regarding education can be explained from a cultural perspective. Australian culture accepts various opinions, respects expertise, and values empiricism. These previously mentioned characteristics of Australian culture can be found in Hofstede (1980). This indicates that Master or PhD degrees are not the prerequisites of experts in Australia. Australian culture focuses more on the ability and practical experience of the experts, and this has been outlined in the discussion within preceding sections of this work. Thus, it is understandable that there is no standard method to train computer forensic investigators, and computer forensic experts are mainly cultivated by undertaking real experience (on-the-job training). Similarly, given the young age of computer forensics as a discipline and the relatively small population of Australia, it is understandable that specific training would be niche.

However, there are some major differences between Australia and Taiwan for educational issues within the field of computer forensics. In Taiwan, as with Australia, there is no standard method to produce computer forensic experts, and there is no organization to certify the qualifications of computer forensic experts. The difference between the two countries is that computer forensic investigators in Taiwan are usually sent overseas for any advanced computer forensic training. There are cultural underpinnings that may be used to explain this. Taiwanese culture traditionally tends to avoid any possible uncertainty (Hofstede 1980). Since the current training methods are acceptable, it is not urgent to set up a national standard. This also infers that Taiwanese culture does not focus on long-term issues, and sometimes ignores the core of the problem. In addition, due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b), Taiwanese culture believes that the developments of science (Western scientific values) are stronger in Western countries. Consequently, it is not surprising that computer forensic experts are sent overseas for what is perceived to be better training. In summary, the differences between Australian and Taiwanese culture cause may different results of educational issues within the field of computer forensics.

Question 18 of the Delphi survey instrument sought to ascertain whether the qualifications of computer forensics experts are accepted within their workplace. In both cases, in Australia and Taiwan, respondents agreed that foreign computer forensic experts are accepted. In Australia, this situation is understandable since Australian culture emphasizes on the expertise of an individual (Hofstede 1980). As long as the individual has excellent knowledge and outstanding skills, his or her nationality is not the primary concern. On the contrary, Taiwanese culture accepts the foreign computer forensic experts for different reason. In the field of science, Taiwanese usually believe foreign experts more than local experts, since the development of science (Western scientific values) is not strong in Taiwan. This situation is mainly caused by the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). In summary, Australian and Taiwanese culture accept foreign computer forensic experts for different reasons. With regards to cooperation between the two countries, this is a positive sign, and will potentially enable an expert from one country to be embedded in a team from another.

Question 20 of the Delphi survey asks the respondents of both countries what they believe the government attitude is towards training and education in the field. For both countries, Australia and Taiwan, it was the respondent's opinion that their government's all show a supportive attitude toward computer forensic educations and/or training. Nevertheless, it is explainable that the governments of Australia and Taiwan support computer forensic education and training for different reasons. As has been established, Australia has a close relationship with the United States of America (Albinski 2001; McLean 2006) and Great Britain (Horne 1964; Goldsworthy 2005), and these two countries have an active research and practitioner community for computer forensics. Thus, it is not surprising that the Australian government can obtain the latest information about computer forensics, which it can then use to make practical decisions. On the other hand, the Taiwanese government does not have such a close relationship with the United States of America and/or Great Britain. In addition, Taiwanese culture does not focus on the value of science (Western scientific values), and always follows the lead of Western countries in the field of science. This situation is mainly caused by the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). This indicates that Taiwanese government does realize that the developments of computer forensics are not perfect. Therefore, it is reasonable for Taiwanese government to place attention on education, training, and research within the field of computer forensics. In summary, the

developments of computer forensics are not ideal in Australia or Taiwan. Therefore, both governments, of course, are willing to support the education, training, and research within the field of computer forensics. However, the reasons that cause these situations are different due to their different cultural backgrounds.

Question 23 of the Delphi survey instrument sought to understand what each country thought the time required to train a computer forensics expert was. The Australian Delphi respondents stated that 2 years is a recommended and reasonable time period to properly train a computer forensic investigator. However, Taiwanese Delphi respondents agreed that 1 year is the minimum requirement for suitable training of a computer forensic investigator. There are cultural explanations for this difference. Australian culture takes a more conscientious and serious attitude to the application of science. This standpoint is supported by the Australian scientific world view proposed by Slay (2000b). However, science (Western scientific values) has a lower level of attached importance and therefore does not obtain enough attention in Taiwanese culture due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). Not surprisingly, a less conscientious answer is provided by the Taiwanese Delphi consensus. In summary, Australian culture treats science applications more seriously than Taiwanese culture. However, this is not to suggest that Taiwanese computer forensics experts are less qualified than Australian experts, but that their minimum training period is potentially shorter. For cooperative purposes between the two countries, there are potential issues in that a Taiwanese analyst may not have the minimum training expected within an Australian environment. However, the chances of this are small, and can be dealt with on a case-by-case basis.

In Question 9 of the case-study interviews, the Australian respondents, ACSE 1 and ACSE 2, both agreed that cross-organizational and cross-disciplinary cooperation is important for improving the future development of computer forensics. Although Australian culture emphasizes the value of exclusive responsibility (Hofstede 1980), this does not prevent cooperation from occurring, especially in areas of research and non-case-specific discussion. On the other hand, the Taiwanese respondents, TCSE 1 and TCSE 2, gave the opinion that this type of cooperation is not utilized as it might be. An understanding of this lack of cooperation may be due to the Taiwanese cultural practice of not focusing on the issues that are not presently urgent (Hofstede 1980). In summary, due to the different natures of Australian culture and Taiwanese culture, they

consider cross-organizational or cross-disciplinary cooperation differently. However, this is not to suggest that the Taiwanese experts are opposed to cooperation merely that less emphasis is placed upon it.

6.5 Law Dimension

This section discusses the Delphi questions and case study interviews related to how each culture understands and relates legislation, the law and legal matters to the field of computer forensics. Given that the law is a factor in every computer forensic investigation, this is an important area of discussion when comparing the two countries in this work. As with the previous sections of this work, each of the results from both the surveys and case study interviews have already been discussed separately and specifically to the individual culture, and this section aims to provide the comparison between the two cultures.

Question 10 and 11 of the case study presented to both cultures solicited information regarding understanding between computer forensic analysts and members of the court in their respective country. Australian and Taiwanese case study participants all agreed that the understanding between computer forensic investigators and members of the court could and should be improved. Interestingly, there is no explicit difference between the Australian and Taiwanese case studies. In addition, the findings of case study Question 11 can be further discussed by combining the results with the outcomes of the Delphi surveys, specifically Question 35 and 36. These results suggested that a potential long term issue with the presentation outcomes of digital evidence results from the fact that members of the court have little or insufficient knowledge of digital evidence. This is true for both Australian and Taiwanese members of court. However, digital evidence is still regarded highly, and given substantial weighting within Australia. The reasons behind this may be that culturally, Australia culture respects dissent and expertise, and this is supported in Hofstede's work (1980). As long as the credibility and validity of digital evidence are proved and provided by computer forensic experts, it is just treated as another type of evidence. On the other hand, digital evidence is given a high weighting only in digital incidents in Taiwan. This means that digital evidence is given a low weighting or is regard as circumstantial evidence in most situations. The cultural underpinning of this may be that traditionally, people in Taiwan tend to care only about their own issues. In this case, they can avoid any possible

uncertainty (Hofstede 1980). Thus, it is not surprising that the importance of digital evidence is ignored by members of the court, as digital evidence is considered an issue belonging to computer forensic experts. In summary, two different outcomes are produced due to different cultures.

From Question 37 of the Delphi surveys, the common outcome discusses in Section 4.2.3.4 and 5.2.3.4 is that Australian common law and Taiwanese laws are designed from two very different perspectives on different societal foundations. Within Australian common law (Cater 1995; Heilbronn *et al* 2002), there is a stage called discovery (Christopher and Hidgekiss 2006; Davies 2006), the purpose of which is for the two opposing parties to exchange relevant evidence before the trial as their obligations in order to seek the prior settlement. On the other hand, there is no such concept in Taiwanese law. The concept of Taiwanese laws focuses on punishment rather than providing an additional opportunity for alternative solutions. The discussion of Taiwanese laws can be found in Poh-Ling (1997). In summary, due to the different natures of Australian culture and Taiwanese culture, laws are designed from different perspectives. From a cooperative perspective between the two countries, the different legal systems may pose a potential issue, as legislative changes cannot be merely mapped out, but as there are different processes and stages in each, more detailed processes are required. It may even be that if an analysis team from one country is working on an international case, they may need to acquire and embed a legal expert from the other country in their team.

Question 38 of the Delphi survey instrument sought to determine if the development of current technology is beyond the current state of law, and if so, to what extent. The results of this work show that the development of the computer forensic technology is occurring faster than the development of legislation to control, shape and understand it. However, there are additional and interesting discoveries for this question. In Australia, Delphi experts stated that this situation does not affect the attitude to their jobs. One interpretation for this is because Australian culture has sound faith in individualism, uniqueness, and independence (Hofstede 1980). Thus, outside factors can rarely affect Australian' thoughts and behaviours. Conversely, Taiwanese experts described that the incompletion of legislation has certain effects on their attitudes towards computer forensic issues. The nature of Taiwanese culture believes more in collectivism than individualism. This argument is corroborated by the finding of Hofstede (1980).

Taiwanese people culturally tend to seek identification within a group. In addition, Taiwanese are more easily affected by outside factors, and their attitudes are changed by these outside variables. In summary, the different findings of this question can be explained from the cultural perspectives involved.

6.6 Personal Preferences and Skills Dimension

This section discusses the Delphi questions and case study interviews related to the respondents' personal preferences and skills. As with the previous sections of this work, each of the results from both the surveys and case study interviews have already been discussed separately and specifically to the individual culture, and this section aims to provide the comparison between the two cultures.

Question 25 of the Delphi survey seeks to understand what the respondents feel the ramifications are of the collisions of hash function outputs. This is an interesting issue from a technical perspective, as the use of a hash system with known collisions may result in challenges to the integrity of any computer forensic analysis. Of the respondents, there is a difference in opinions between the Australian and Taiwanese experts. The Australian Delphi experts did not believe that the collisions of hash functions are able to affect the outcomes of computer forensic investigations since the possibility of collision is too low. Culturally, this may be explained by the tolerance that is part of Australian culture. This argument is supported by the finding of Hofstede (1980). The Australia Delphi experts do not believe that collisions of hash functions are a serious problem, and this may be due to their very low probability. Thus, they do not need to seek for an absolute answer (e.g. perfect hash function) since an acceptable answer (e.g. using multiple hash functions) exists. On the contrary, the Delphi survey indicated that the Taiwanese respondents believe that the collision of hash functions has potential impact within the field. Potentially, collisions within hash functions make the digital evidence less robust. Culturally, this may be because Taiwanese people are used to seeking an unambiguous answer for a problem (Hofstede 1980). They would like to make sure there is no problem for the collisions of hash functions. In summary, although using multiple hash functions is recommended in both Australia and Taiwan, Australian and Taiwanese Delphi respondents answered Delphi Question 25 by different beliefs.

Question 39 and 40 of the Delphi survey instrument, and Question 12 of the case study interviews asked respondents about data-wiping and encryption within their work. These found that the use of data wiping and data encryption tools for digital data is different in Australia and Taiwan, and that the answers to why this is may be cultural. Australia is a country with less competition. Thus, it is understandable that Australian culture is typically leisurely and relaxed (Horne 1964). This indicates that people in Australia usually do not believe that there is an urgent need for prevention and protection. On the contrary, people in Taiwan live in a more competitive environment. This is because the available resources are less than the population. Therefore Taiwanese people must compete for better results. In addition, Hofstede (1980) stated that "*Higher anxiety and stress are experienced.*" is a typical characteristic of a strong uncertainty avoidance society. According to his classification, Taiwanese culture has strong uncertainty avoidance. Consequently, people in Taiwan realize the importance of protection and prevention. In conclusion, Australian and Taiwanese show two different attitudes for the use of data wiping and data encryption tools due to their indigenous cultures.

Question 13 of the case study interview is designed to elicit information regarding the ways used to upgrade the professional skills of computer forensic investigators in Australia and Taiwan. The outcome of this indicates that the methods used are the same in both countries. These include, for both Australia and Taiwan, attending national or international conferences and vendor-based computer forensic courses as two well-accepted methods for advanced training methods. However, there are some additional findings between the opinions provided by Australian and Taiwanese case study participants. Australian computer forensic experts stated one interesting standpoint, describing that the ability of an individual is more important than his or her educational qualifications. This shows that Australian culture values the importance of empiricism (Hofstede 1980). This has been touched upon in the analysis of other questions arising from the Delphi surveys and interviews in previous dimensions. In addition, Taiwanese case study participants expressed the view that sending computer forensic investigators overseas is one of their major training methods. This situation indicates that Taiwanese culture normally follows the lead of Western countries within the field of science. This has also been touched upon. This argument is understandable due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). In summary, case study Question

13 discovers the different attitudes toward the skills of a computer forensic investigator between Australia and Taiwan.

6.7 Characteristics of Australian and Taiwanese Culture

Delphi surveys and case studies conducted in Australia and Taiwan demonstrate that there are some differences between these two cultures. Table 20 shows the characteristics of Australian and Taiwanese culture discovered by this research.

Table 20: Characteristics of Australian Culture and Taiwanese Culture

	Australia	Taiwan
Tolerance	More tolerant of different standpoints on issues	Less tolerant of different standpoints on issues
Uncertainty Avoidance	Less uncertainty avoidance	More uncertainty avoidance
Acceptance of Ambiguity	More acceptance of ambiguity	Less acceptance of ambiguity
Expertise	Emphasis more on expertise	Emphasis less on expertise
Experience	Emphasis more on experience	Emphasis less on experience
Autonomy	More autonomy	Less autonomy
Independence	More independent	Less independent (More dependent)
Group Identification	Less group identification (more autonomy)	More group identification (less autonomy)
Philosophy of Education	Range of models	Confucianism is the main trend
Value of Western Science	Australian culture accepts and develops Western science	Taiwanese culture usually follows the lead of the West in its science
Accessible of Workplace Supervisor	Australian culture views workplace hierarchy as an arrangement for convenience	Taiwanese culture interprets workplace hierarchy rigidly and as one which specifies inequality
Major Cultural Trend	Easy, relaxed, and comfortable	Competitive

6.8 Summary of this Chapter

This chapter combines Australian findings, including Delphi survey and two case studies, with Taiwanese findings, including Delphi survey and two case studies, in order to provide an overall understanding of the cultural differences within the field of computer forensics between Australia and Taiwan.

Each of the dimensions discussed raised some interesting comparisons, and these will be discussed in turn. The first of these dimensions, the Current Situation Dimension, found several interesting facts and comparisons. Namely:

- The differences between Australian and Taiwanese culture are able to explain how each country understands the field of computer forensics. The underlying understanding of the field of science for these cultures changed how experts from these countries see the field of computer forensics.
- Australian culture emphasizes the value of scientific implementations, and this is reflected in research, specifically when the outcome is implementation-based. However, Taiwanese culture tends to focus on the short-term objectives.
- Taiwan and Australia consider the trustworthiness and reliability of meta-data differently from each other, and this outcome is potentially important to any cooperation between the two countries, or where these cultures intersect. Australians place a higher value on meta-data than Taiwanese computer forensic experts, and this has potential consequences in cross-jurisdictional operations.
- Australia and Taiwan have different attitudes towards the relationships between the fields of computer security and computer forensics. In Australia, computer security and computer forensics are considered two entirely different fields of study, and although a relationship is discussed, it is considered a distinct discipline within itself. Taiwanese experts believe in a much closer relationship between computer security and computer forensics.
- Whilst issues of date and time are recognized to be important in both Australia and Taiwan, two cultures treat time issues from different perspectives. Given the complexity of Australian time, having both multiple time zones and daylight saving, further work may be required if experts from another country examine evidence originating in Australia.
- Both Australia and Taiwan encounter similar, relatively low amounts of encrypted data in investigations. Whilst there are many explanations for this, there are certainly cultural influences that impact these numbers.
- Australian and Taiwanese culture adopts different methods to evaluate the ability of an individual and this may be reflected in their choice of computer forensic analysts.

The Current Situation Dimension brought up a number of interesting similarities and differences. However, even then there are similarities in the data presented; the countries often arrived at the same conclusion through different cultural decisions. The most marked of these is how Australia and Taiwan understand and perceive the nature of Science.

The second dimension, the Policy and Organization Dimension, also raised a number of similarities and disparities, both based on how the field of computer forensics is organized externally and internally, but also how it is governed. Specifically, this dimension discovered that:

- Australia and Taiwan have different structures in place for policing; this is born out of different overall policing structures and organizations.
- Neither Australia nor Taiwan outsource their forensic analysis, but the reasons behind this are different, and there is a cultural aspect.
- Whereas Australia has multiple policing agencies and jurisdictions, each dealing with electronic evidence, Taiwan has a central computer forensic laboratory that analyses all computer forensic evidence within the country.
- Whereas Australia seeks to foster relationships with local universities and academia, Taiwan has a greater respect for experts that originate from other countries.

Again, this work has shown that whilst there is a number of similarities between the state of policy and organization between Australia and Taiwan, these are the result of different cultural underpinnings and perspectives. There are also some very large differences between the two countries, and much of this organizational variation comes from a combination of geographic and cultural differences.

The comparisons of the third dimension, the Education Dimension, between Australia and Taiwan were interesting in how markedly different the outcomes were. These were not just different from a perspective of educational programs, but that different qualities and experience levels were prized. Specifically:

- In Taiwan, as with Australia, there is no standard method to produce computer forensic experts, and there is no organization to certify the qualifications of computer forensic experts.
- Whereas Australian computer forensic teams provide much of an individuals training in-house, Taiwanese teams will often send analysts and investigators overseas for advanced work.
- Australian and Taiwanese cultures both accept foreign computer forensic experts and respect external training, although this is for different reasons.
- Whilst Australian respondents feel that it takes two years to train a forensic analyst, the Taiwanese respondents felt one year was an appropriate training period. This is related to the way that these two cultures perceive science.
- The different natures of Australian culture and Taiwanese culture consider cross-organizational or cross-disciplinary cooperation differently. This is not to suggest that the Taiwanese experts are opposed to cooperation, merely that less emphasis is placed upon it.

As can be seen by this summary, the Australian and Taiwanese cultures perceive education very differently from each other. Whilst this is not a negative thing, it must be dealt with and understood in any international communication and cooperation.

The Law Dimension sought to compare and contrast how each culture understands and relates legislation, the law and legal matters to the field of computer forensics. This was not expected to be a simple task, given the different legal systems and histories between the two countries. This work specifically discovered that:

- Both Australian and Taiwanese case study participants agreed that the understanding between computer forensic investigators and members of the court could and should be improved. Again, whilst the outcome was the same from both surveys, the cultural perspectives differed.
- Australian common law and Taiwanese laws are designed from two very different perspectives on different societal foundations. The differences are so extreme that these cannot be easily mapped, as there is a number of stages and process in each that the other lacks.
- Both Australian and Taiwanese experts revealed that they believed that current technology is evolving much faster than the legislation designed to control it.

However, the cultural principles behind the responses from the two countries were based on different societal precepts.

Given the differing legislation, there is a large amount of agreement with the respondents in this section. However, the underlying cultures are different, and some of these similarities are based on different perspectives.

The Personal Preference and Skills Dimension was the last dimension, and as with the other dimensions, this work brought out some interesting similarities and disparities between Australia and Taiwan. However, in all cases, the cultural discussion and reasoning affecting the decision is the most interesting comparison. This final dimension elicited some interesting comparisons, namely:

- Whilst Australian experts do not feel the issue of hash functions with collisions is a serious issue, the Taiwanese Delphi survey respondents see it as a potential future issue.
- Data-wiping and encryption on work is used by more experts in Taiwan than in Australia. People in Taiwan live in a more competitive environment and therefore realize the importance of protection and prevention.
- Both Australia and Taiwan attempt to upgrade the skills of analysts by attending national or international conferences and vendor-based computer forensic courses.

Again, the cultural differences are large, even in such an international field as computer forensics.

In addition to the information that can be directly compared from these dimensions, the discussions in this chapter show that two different cultures indeed have impact on the field of computer forensics. 42 out of 53 questions, including 30 Delphi questions and 12 case study questions, are able to prove this statement, by providing a cultural insight that differs between the two countries. It is only 11 questions, consisting of 10 Delphi questions and 1 case study question, that had no cultural bias at all and are therefore based on global values, and are beyond the influence of culture. In short, the discussions listed in this chapter confirm the research question of this thesis.

7 Conclusion

7.1 Overview of this Chapter

This, the final chapter of the research, seeks to draw insight from the research and relate this back to answering the high-level questions that were originally posed in Section 1.4. As discussed, the overarching question of this work is:

'*Does Culture have an impact on Computer Forensics Processes and Applications?*'

This research question was then partitioned into a number of sub-questions, which, if all answered, would therefore answer the original research questions. These sub-questions are:

- Does culture have an impact on current conditions of computer forensics?
- Does culture have an impact on policy and organization of computer forensics?
- Does culture have an impact on education and training within computer forensics?
- Does culture have an impact on legal issues of computer forensics?
- Does culture have an impact on the personal preferences and skills of computer forensic practitioners?

Discussion of the research outcomes ensures that the original question has been answered fully, and therefore these questions will be discussed and link to throughout this chapter. Additionally, this chapter identifies future areas of research that the outcomes of this research point to.

Section 7.2 discusses the findings of the Australian studies, which consisted of a Delphi survey instrument and two case study interviews. The Delphi survey had eight computer forensic expert participants, including five academic researchers and three computer forensic practitioners, and the case study component of this work interviewed two computer forensic practitioners. These ten distinct experts provided their unique opinions as the valuable information to evaluate the role of Australian culture within the field of computer forensics. Whilst this was discussed in Chapter 4, a summary of the findings and cultural underpinnings is a relevant outcome of this work and assists in answering the research questions posed.

Section 7.3 introduces the Taiwanese Delphi survey and two Taiwanese case study interviews. Delphi consensuses were made by ten computer forensic experts, and

outcomes of two case study interviews were provided by two computer forensic practitioners accordingly. This indicates that there were twelve distinct Taiwanese computer forensic experts helped the achievements of this thesis. Again, whilst this work has been independently discussed in Chapter 5, the outcomes are relevant to answering the original research questions posed.

In Section 7.4, the cultural interpretations of Australian studies are discussed with the cultural explanations of Taiwanese studies. These comparisons are able to demonstrate that culture is not a universal concept, and further support the fact that different cultures have influence on applications of computer forensics. This standpoint is able to answer the major research question. Taking the results from Chapter 6 and comparing it with the original questions is the major focus of this work, and therefore explanation is required.

Section 7.5 provides suggestions for the future cooperation between Australia and Taiwan based on the outcomes of this work and an understanding of the different fundamental cultural underpinnings. The understanding of cultural differences between Australia and Taiwan is helpful for improving the cross-national collaboration.

Section 7.6 continues this by suggesting several future areas of research that extend upon the outcomes of this work. This work includes extending the outcomes, adapting the fields, expanding the context and also adding more analysis to different cultures.

Lastly, Section 7.7 provides an overall understanding of this research and shows the conclusion of this thesis by describing that the findings of Australian and Taiwanese studies and their cultural interpretations.

7.2 Culture of Australian Computer Forensic Results

7.2.1 Australian Data Collection

Chapter 4 of this research attempted to discover several aspects of the methodologies and organization of Australian computer forensic experts, so as to understand the Australian culture within the field. From this, the several aspects of the research sub-

questions may be answered. An understanding of the Australian computer forensic culture provides a basis for comparison for other cultures.

In Australia, eight computer forensic experts participated in the Delphi survey, and provided their valuable and professional opinions for Delphi consensuses. In addition, two Australian case study interviews were conducted with the participation of ACSE 1 and ACSE 2. They provided their insights for current computer forensic conditions based on their actual experiences. The findings gathered by the previous two research methods are listed in Section 7.2, and used as the fundamental arguments in this research to further evaluate the Australian cultural attitudes toward applications of computer forensics. Section 7.2.7 of this research explains that the discoveries of Australian studies actually answers several aspects the five sub-questions mentioned in Section 1.4, as they relate to the Australian cultural context. Section 7.4 concludes this research, and gives final discussion on the overall research question, the answers produced and a final discussion on this study.

The findings of Australian Delphi survey and two case study interviews also demonstrate that some values within the field of computer forensics are beyond the influence of culture. The results of Delphi Question 4, 6, 8, 9, 12, 24, 26, 29, 30 and 31, and case study Question 3 are able to prove this statement. These 11 questions show that culture does not have effect on the basic concepts and essential understanding of technical issues. Thus, these 11 questions are not going to be discussed in this section.

7.2.2 Australian Outcomes of the Current Situation Dimension

In the Current Situation Dimension, several cultural standpoints were revealed from both the Delphi survey instrument and the case study interviews. Australia has a similar cultural background to other Western countries (Albinski 2001, Horne (1964). Australia's relationship with other western countries allows it, as a country, to obtain the latest results of computer forensics with relative ease. In addition, according to Slay (2000b), a scientific worldview is a large part of Australian culture. This shows that the value of science obtains attentions in Australian culture. Lastly, the discoveries in this dimension also show that Australian culture has several characteristics; individualism (Hofstede 1980), accepting of dissent, and relaxation (Horne 1964). Also, empiricism and the ability of an individual are very important within Australian culture. There are

also potential logistical issues in the form of multiple time zones and multiple Daylight Saving times. These characteristics of Australian culture have certain effects on the applications of computer forensics.

7.2.3 Australian Outcomes of the Policy and Organization Dimension

In Policy and Organization Dimension, several cultural perspectives were discovered from both the Delphi surveys and the case study. These Australian cultural standpoints are supported by Hofstede's research results (1980). The first cultural perspective is that Australian culture emphasizes the value of individualism and independence. This perspective is found in both the Delphi surveys and in the case studies. The second cultural explanation is that Australian culture allows the existence of different opinions. Lastly, the third cultural account describes that Australian culture does not underline the hierarchy. In short, the previous three cultural explanations are the factors that are able to affect the results of the questions in this dimension.

7.2.4 Australian Outcomes of the Education Dimension

There were six cultural explanations found by the questions in Education Dimension. Besides the first cultural explanation, the other four are corroborated by Hofstede's research results (1980).The first cultural perspective is that Australia can obtain innovative results of computer forensics from the United States of America and Great Britain as Australia has close relationship with these countries and also has similar cultural background to them (Horne 1964; Albinski 2001; Goldsworthy 2005; McLean 2006). The second cultural viewpoint is that the different opinions are acceptable. The third cultural account describes that the empiricism is a very important concept within Australian culture. The fourth cultural standpoint shows that Australian culture emphasizes the value of expertise and the ability of an individual. This perspective can be independently confirmed as both the Delphi surveys and the case study respondents had this outcome. The case study also found that individualism is highly prized in the Australian computer forensic culture. Lastly, the sixth cultural perspective points out that tolerance is a concept that cannot be forgotten in Australian culture. In summary, the Delphi surveys and the case study in this dimension discovered the above six cultural explanations for the applications of computer forensics.

7.2.5 Australian Outcomes of the Law Dimension

Delphi questions in Law Dimension reveal 4 cultural perspectives. The first cultural perspective points out that Australian culture values the concept of tolerance (Hofstede 1980). The second cultural explanation describes that expertise is respected in Australian culture (Hofstede 1980). The third cultural viewpoint shows that Australian culture believes that the nature of humanity is virtuous (Horne 1964). Lastly, the fourth cultural standpoint describes that Australian culture values the individualism and independence (Hofstede 1980). This is supported by the findings of Question 10 and 11 of the case study, which confirm that empiricism and individualism are two important values within Australian culture. In conclusion, the Delphi questions and the case study outcomes confirm that the applications of computer forensics are affected by Australian culture in this dimension.

7.2.6 Australian Outcomes of the Personal Preferences and Skills Dimension

In the Personal Preferences and Skills Dimension, tolerance and relaxation (Horne 1964) are two cultural factors to explain the findings of the Delphi questions. This is confirmed by the case study, which discovered that the Australian living style is comfortable and relaxed (Horne 1964). The case study also showed that Australian culture puts emphasis on expertise and ability of an individual. This situation corroborates the relationship between culture and the applications of computer forensics. This shows that the applications of computer forensics are not a culture-free issue.

7.2.7 The Relationship between the Australian Results and the Research Questions

An understanding of the Australian culture in the computer forensic field is vital in being able to understand and measure the differences between the cultures in other countries. The discussion given in these components is broken down in the dimensions used, and is based on the aspects of the research sub-questions; current conditions, policy and organization, education and training, legal issues and personal preferences and skills.

According to the discussions of Section 7.2, this section confirms the relationship between the results of Australian studies, consisting of Delphi findings and case study outcomes, and the five research sub-questions. The findings of Australian studies show that the applications of computer forensics are deeply related to the Australian culture. This further indicates that the Australian culture is one of the factors to affect the applications of computer forensics.

The following paragraphs show that the five sub-questions are satisfied as well. In Current Situation Dimension, the Australian research findings indicate that the current conditions within the field of computer forensics are affected by the characteristics of Australian culture. For example, the attitude of Australian government toward computer forensics is one of the discoveries that is able to support this statement. This means the sub-question, *Does culture have an impact on current conditions of computer forensics?*, is satisfied within the Australian context. The extent of this cultural impact will only be known with comparison.

In Policy and Organization Dimension, the Australian research findings show that the computer forensic policies and organizations are influenced by the uniqueness of Australian culture. For example, the policies of computer forensic readiness and the hierarchical design of the computer forensic organizations can support this argument. In short, the sub-question, *Does culture have an impact on policy and organization of computer forensics?*, is satisfied within the Australian context.

In the Education Dimension, it is realized that the educational programs within the field of computer forensics are shaped by the Australian culture. For instance, the Australian research findings show that the ability of a computer forensic investigator is emphasized, and this discovery is able to support this standpoint. In summary, the sub-question, *Does culture have an impact on education and training within computer forensics?*, is satisfied within the Australian context.

In the Law Dimension, the relationship between legal issues and computer forensics is verified by Australian studies. For example, due to the characteristics of Australian culture, the court does not have many problems to accept the use of digital evidence. This means that the sub-question, *Does culture have an impact on legal issues of computer forensics?*, is satisfied within the Australian context.

In the Personal Preferences and Skills Dimension, the findings of this thesis show that Australian culture is able to influence the computer forensic experts' preferences and their attitudes toward computer forensic skills. For example, Australian studies show that the computer forensic experts' unique attitudes toward the collisions of hash functions, and this discovery is a good illustration to support the previous standpoint. This circumstance further infers that the sub-question, *Does culture have an impact on the personal preferences and skills of computer forensic practitioners?*, is satisfied within the Australian context.

In summary, the results of Australian studies not only prove the relationship between Australian culture and the applications of computer forensics, but also fulfil the major research question and five subsequent questions. However, the questions cannot be completed within itself just from the Australian context, but the nature and extent of the cultural impacts can be discovered through comparison with the Taiwanese results. However, by discussing each culture independently, the nature can be solidified from the outcomes.

7.3 Culture of Taiwanese Computer Forensic Results

7.3.1 Taiwanese Data Collection

Chapter 5 of this research attempted to discover several aspects of the methodologies and organization of Taiwanese computer forensic experts, so as to understand the Taiwanese culture within the field. From this, the several aspects of the research sub-questions may be answered. An understanding of the Taiwanese computer forensic culture provides a basis for comparison for other cultures.

This section lists the cultural findings of Taiwanese studies, including the Delphi survey and two case study interviews, in Section 7.3. There were ten computer forensic experts participated in the Delphi survey, and two computer forensic practitioners were willing to provide their professional opinions for the case study interviews. The researcher is able to interpret the Taiwanese cultural attitudes toward applications of computer forensics based on the opinions provided by these twelve computer forensics experts. In addition, Section 7.3.7 explains that the discoveries of Taiwanese studies actually satisfy with the five sub-questions mentioned in Section 1.4.

After conducting Taiwanese Delphi survey and two Taiwanese case study interviews, the researcher conclude that the results of Delphi Question 4, 6, 8, 9, 12, 24, 26, 29, 30 and 31, and case study Question 3 are beyond the influence of culture. This situation shows that the basic concepts and essential understanding of technical issues are culture-free factors. Thus, these 11 questions are not going to be discussed in this section.

7.3.2 Taiwanese Outcomes of the Current Situation Dimension

In the Current Situation Dimension, four cultural standpoints were revealed from the Delphi survey and the case study interviews. Some of these cultural outcomes are consistent with in the work of Hofstede (1980). The value of science is not respected in Taiwanese culture. Within the field of science, Taiwanese culture used to follow the lead of Western countries (e.g. the United States of America). The explanation can be found in the discussions of Delphi Question 1, 2, and 3. The second cultural standpoint shows that Taiwanese culture focuses on short-term objectives, and tends to avoid uncertainties (Hofstede 1980). This outcome is based on both the outcomes from the Delphi survey as well as from the case study respondents. The third cultural perspective finds that, from the Delphi outcomes, Taiwanese culture is usually seeking the unambiguous answer (Hofstede 1980). The final cultural explanation or this dimension, based on outcomes from the case study, shows that Taiwanese culture respects the value of examination (Haifeng 2006). In conclusion, these characteristics of Taiwanese culture have certain effects on the applications of computer forensics.

7.3.3 Taiwanese Outcomes of the Policy and Organization Dimension

In the Policy and Organization Dimension, the Delphi survey responses and the findings of the case study interviews show a number of cultural perspectives that influence the applications of computer forensics. The findings of Hofstede (1980) are able to directly corroborate several of these cultural explanations, and are consistent with the others. The first cultural standpoint shows that the values are different from the in-group and out-group. This also infers that interpersonal relationship is very important in Taiwanese culture. The second cultural perspective points out Taiwanese culture usually focuses on short-term rather than long-term objectives. This also means that Taiwanese culture tends to avoid uncertainties and dislikes change. This outcome is both from the

case study and the Delphi survey instrument. The third cultural discovery is that the value of the science (Western science) is not respected in Taiwanese culture due to the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). Thus, Taiwanese culture usually follows the lead of Western countries (e.g. the United States of America) within the field of science. Lastly, the fourth cultural reason is that Taiwanese culture respect the concept of hierarchy. In short, the discoveries confirm that Taiwanese culture has an impact on applications of computer forensics within the Taiwanese cultural context.

7.3.4 Taiwanese Outcomes of the Education Dimension

In the Education Dimension, the findings of the Delphi questions show that Taiwanese culture does not respect the value of science, and is usually focus on the short-term objectives. This is because Taiwanese culture accepts Confucianism (Jingpan 1990) as the major educational trend, and tends to avoid possible uncertainties (Hofstede 1980).

The case study interviews revealed three cultural factors. Besides the third cultural explanation, the first two cultural features can be found and are supported by Hofstede (1980). The first cultural interpretation states that Taiwanese culture puts more attentions on short-term objectives. The second cultural explanation shows that the unambiguous answer is respected in Taiwanese culture. Lastly, due to the influence of Confucianism, the value of science (Western science) is not emphasized by Taiwanese culture (Jingpan 1990; Ho 1991). Thus, Taiwanese culture usually follows the lead of Western countries (e.g. the United States of America) within the field of science. In short, the findings of this dimension confirm the relationship between Taiwanese culture and applications of computer forensics within the Taiwan.

7.3.5 Taiwanese Outcomes of the Law Dimension

In the Law Dimension of this work, focusing on short-term objectives and believing collectivism are two explicit characteristics of Taiwanese culture, and these two cultural features are supported by Hofstede's research findings (1980). In addition, focusing on short-term objectives further infers that Taiwanese culture tends to prevent uncertainties from occurring. In summary, applications of computer forensics are not isolated from

the cultural influence. These outcomes come from both the Delphi survey instrument as well as the case study.

7.3.6 Taiwanese Outcomes of the Personal Preferences and Skills Dimension

In the Personal Preferences and Skills Dimension, four Taiwanese culture characteristics are discovered. The first cultural perspective is that the unambiguous answer is well-accepted in Taiwanese culture. The second cultural standpoint indicates that people in Taiwan culture tend to protect themselves in any possible way due to their living style and environment. This trait is related to the finding from the case study that people in Taiwanese culture tend to protect themselves in any possible way due to their living style and environment. These three cultural traits are confirmed by Hofstede (1980). In addition, Taiwanese culture does not emphasize the value of science (Western science) because of the influence of Confucianism (Jingpan 1990; Ho 1991; Slay 2000b). In conclusion, the applications of computer forensics are affected by the uniqueness of Taiwanese culture.

7.3.7 The Relationship between the Taiwanese Results and the Research Questions

An understanding of the Taiwanese culture is vital in being able to understand the forensic computing field and in being able to measure the differences between this culture and that in other countries. As with the previous questions, the discussion given in these components is broken down in the dimensions used, and is based on the aspects of the research sub-questions; current conditions, policy and organization, education and training, legal issues and personal preferences and skills. In answering these sub-sections, the research questions may be partially answered.

The following paragraphs show that the five sub-questions are satisfied by the findings of this thesis as well. In the Current Situation Dimension, the findings of Taiwanese studies show that the current conditions within the field of computer forensics are affected by the characteristics of Taiwanese culture. For example, the Taiwanese cultural attitude toward computer forensic SOPs are able to support this viewpoint. This

infers that the sub-question, *Does culture have an impact on current conditions of computer forensics?*, is satisfied within the Taiwanese context.

In the Policy and Organization Dimension, according to the Taiwanese research findings, the computer forensic policies and organizations are influenced by the uniqueness of Taiwanese culture. For example, the policies of computer forensic readiness and the interactions between different organizations are two factors which can explain this perspective. In short, the sub-question, *Does culture have an impact on policy and organization of computer forensics?*, is satisfied within the Taiwanese context.

In the Education Dimension, the educational issues within the field of computer forensics are demonstrated to be associated with Taiwanese culture. For instance, a computer forensic expert is usually sent overseas for the advanced educational program or training. This indicates that the sub-question, *Does culture have an impact on education and training within computer forensics?*, is satisfied within the Taiwanese context.

In the Law Dimension, this thesis reveals the relationship between legal issues and computer forensics. For example, the relationship between the development of computer forensic technology and the development of the current law is one of the novel discoveries of this research. In addition, this discovery is further used to discover the attitudes of computer forensic experts toward the imperfection of legislation. This situation indicates that the sub-question, *Does culture have an impact on legal issues of computer forensics?*, is satisfied within the Taiwanese context.

In the Personal Preferences and Skills Dimension, Taiwanese studies show that the computer forensic experts' preferences and their attitudes toward computer forensic skills are indeed specific to Taiwanese culture. For example, Australian studies show that the computer forensic experts' unique attitudes toward the use of data wiping and encryption tools. This finding is a influential illustration for the previous viewpoint. This circumstance also infers that the sub-question, *Does culture have an impact on the personal preferences and skills of computer forensic practitioners?*, is satisfied within the Taiwanese context.

In summary, the results of Taiwanese studies discover two standpoints which are close to each other. The first standpoint is that the relationship between Taiwanese culture and the applications of computer forensics is confirmed. In addition the second standpoint is that the five sub-questions are fulfilled. However, the questions cannot be completed within itself just from the Taiwanese context, but the nature and extent of the cultural impacts can be discovered through comparison with the Australian results. However, by discussing each culture independently, the nature can be solidified from the outcomes. At this point, it can be seen that there are differences between the two cultures, but a more in-depth analysis can see where the differences are, their extent, and where values are more global.

7.4 Results of Major Research Question and Interpretations for Cross-Cultural Applications of Computer Forensics

From the discussion in Section 7.2.7 and 7.3.7 of this work, the five research sub-questions can be partially proven correct within both the Australian and Taiwanese contexts. The research questions ask whether culture affects the field of computer forensic in the two countries, and the results from the Delphi surveys and the case study interviews are able to quantify this.

This section of the thesis further confirms the following standpoints: Australian culture and Taiwanese culture are different from each other and have different understanding of the world, and that the relationship between different cultures and applications of computer forensics. This means that the main research question, *Does Culture have an impact on Computer Forensics Processes and Applications?*, can be considered satisfied. Both the Australian and Taiwanese cultural outcomes are different, which supports the research standpoints raised. As the research question is comprised of the five sub-questions, and each of these can be seen to be answered, the overall research question can be verified for both the Australian and Taiwanese cultures.

However, this research is able to expand upon the research question, and not only state that culture does affect computer forensic, but can further quantify these changes for the two cultures analysed. This section of the research lists the characteristics of Australian and Taiwanese cultures which causing the different outcomes of computer forensic applications in Australia and Taiwan.

The major characteristics of Australian culture within the field of computer forensics discovered by this research can be quantified as the following:

- Australian culture is tolerant of different opinions.
- Australian culture is willing to take on the challenge of, and face the possible uncertainty of, the future.
- Australian culture emphasizes on the expertise.
- Australian culture emphasizes on the experience.
- Australian culture puts emphasis on the initiative and achievement of an individual.
- Australian culture respects the value of independence.
- Australian culture respects the value of autonomy.
- Australian culture views the hierarchy as the arrangement for convenience.
- Australian culture believes everyone has equal right, and the supervisor is accessible.
- Australian culture shares very similar cultural background with the United States of America and Great Britain.
- Australian culture believes the value of science.
- Australian culture is easy, relaxed, and comfortable.

By comparison, the Taiwanese computer forensic culture is markedly different. The major characteristics of the Taiwanese computer forensic culture discovered by this thesis are listed as follows:

- Taiwanese culture accepts Confucianism as major educational trend.
- Taiwanese culture does not emphasize the value of science (Western science).
- Taiwanese culture emphasizes the value of examination.
- Taiwanese culture follows the lead of Western countries in the field of science.
- Taiwanese culture seeks for the unambiguous answer.
- Taiwanese culture focuses on short-term objectives.
- Taiwanese culture is not willing to take the challenges, and tries to avoid possible uncertainty in the future. '*What is different is dangerous*' is believed.
- Taiwanese culture seeks the identification within the group.

- Taiwanese culture believes there are different values between in-group and out-group.
- Taiwanese culture interprets the hierarchy as the nature of inequality.
- Taiwanese culture believes that the supervisor is inaccessible.
- Taiwanese culture is competitive.
- There are some fundamental differences between these two cultures, both in general and as they apply to the field of computer forensics. These differences occur at all levels, the current situation, policy and organization, education and training, legal issues and personal preferences and skills. These differences relate to all areas, but with some organisation they do not preclude international cooperation. Once known, such differences may be noted and organized.

7.5 Suggestions for Cross-Cultural Cooperation between Australia and Taiwan

The core concept of this research question is to seek the relationship between culture and applications of computer forensics. After conducting Australian and Taiwanese Delphi surveys and case study interviews, this relationship is established and confirmed. In addition, this thesis proposes useful suggestions for the future academic and/or criminal cooperation between Australia and Taiwan within the field of computer forensics.

The foremost concept for the Australian and Taiwanese computer forensic researchers and practitioners is that people in Australia and Taiwan have completely different thought, thinking, behaviours, attitudes, and cultural backgrounds. This means Australian computer forensic experts need to tolerate Taiwanese culture and methods, and vice versa. Open-mindedness is the basic understanding for a cross-cultural cooperation, and is very helpful as well. The following three sections introduce more specific suggestions for the cooperation between Australia and Taiwan. The suggestions are classified into three categories. In Section 7.5.1, suggestions for Australian computer forensic experts are given, and Section 7.5.2 lists the suggestions for Taiwanese computer forensic experts. In addition, Section 7.5.3 presents the suggestions for both Australian and Taiwanese computer forensic experts by 5 dimensions.

7.5.1 Suggestions for Australian Computer Forensic Experts

This section discusses the situations that may occur in a cross-cultural cooperation between Australia and Taiwan, and provides useful suggestions for an Australian computer forensic expert when he or she is a member or a manager of a cross-cultural team.

If an Australian computer forensic expert is a manager or a member of a cross-cultural team, he or she should contact with the senior Taiwanese computer forensic experts or the manager when there are decisions need to be made. This is because the relationship between the supervisor and the subordinate is respected in Taiwanese culture. The supervisor has the absolute right to make the decision. On the other hand, the subordinate can only follow the orders provided by his or her boss. Thus, Australian computer forensic experts need to understand that the supervisor must make the decisions in Taiwanese culture. A supervisor has legitimate power to make important decisions.

If an Australian computer forensic expert works as a manager or a member of a cross-cultural team, he or she should give orders as clearly as possible when he or she is authorized. In Taiwanese culture, people have little trouble in accepting orders from an authorized person (e.g. the supervisor). Clearer orders can help Taiwanese computer forensic experts to avoid ambiguous situations. This indicates that if an authorized Australian computer forensic expert tries to avoid giving directions, he or she can make the work situation difficult. It is better for an Australian computer forensic expert to provide an unambiguous order, if he or she is authorized.

If an Australian computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that the concept of collectivism is well-accepted in Taiwanese culture. This phenomenon indicates that the performance of an individual is not emphasized in Taiwanese culture, and the competition between colleagues is not encouraged either. Seeking identification within a group is very important within Taiwanese culture. Instead of focusing on the diverseness of members of a cross-cultural team, an Australian computer forensic expert should concentrate on the performance of the whole group.

If an Australian computer forensic expert works as a manager or a member of a cross-cultural team, he or she should comprehend that specific rules or regulations are emphasized in Taiwanese culture. A clear instruction is helpful for most situations when Taiwanese computer forensic experts are involved. In this case, possible misunderstandings (between Australian and Taiwanese computer forensic experts) can be ruled out, and mutual trust (between Australian and Taiwanese computer forensic experts) can be established. Following the rules and orders is an important part of Taiwanese culture. In summary, an Australian computer forensic expert should realize that specific rules may direct affect the success or failure of a cross-cultural cooperation.

If an Australian computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that the interpersonal relationship plays a significant role in Taiwanese culture. This situation further infers that negotiating is more important than arguing for disputes or different opinions. The concept of individualism is very hard to be implemented in Taiwanese culture. Working as a team or working with colleagues is the major trend in Taiwanese culture. In short, an Australian computer forensic expert has to understand the importance of interpersonal relationship and teamwork in Taiwanese culture.

If an Australian computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that the concept of hierarchy is respected in Taiwanese culture. The relationship between a supervisor and a subordinate is very important in Taiwanese culture, and the supervisor should be esteemed by the subordinate. Moreover, this situation also infers that interpersonal relationship plays an important role in Taiwanese culture. In summary, an Australian computer forensic expert should put more attention on civility and respect when he or she has Taiwanese supervisors and/or colleagues.

If an Australian computer forensic expert works as a manger or a member of a cross-cultural team, he or she should realize that Taiwanese culture emphasizes the unambiguous answer for a problem. This means an exact solution is the ultimate goal of a computer forensic investigation. Presenting several possible results is not a well-accepted way in Taiwanese culture. Seeking the only truth is important in Taiwanese culture. This is different from Australian culture that allows the existence of various

opinions. In summary, an Australian computer forensic expert should comprehend the value of the unambiguous answer within Taiwanese culture.

7.5.2 Suggestions for Taiwanese Computer Forensic Experts

This section discusses the situations that may occur in a cross-cultural cooperation between Australia and Taiwan, and provides useful suggestions for a Taiwanese computer forensic expert when he or she is a member or a manager of a cross-cultural team.

If a Taiwanese computer forensic expert works as a manger or a member of a cross-cultural team, he or she should realize that questions and challenges are the ways Australian computer forensic experts seek the answers to a problem. They do not challenge the leadership of the manager by asking questions or pointing out drawbacks. In fact, questions and challenges are well-accepted methods for seeking answers to a problem, and do not mean anything else. In short, a Taiwanese computer forensic expert should realize that different methods are used by Australian computer forensic experts in seeking the answers to a problem.

If a Taiwanese computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that the every individual is considered and treated differently in Australian culture. Individualism is a well-accepted concept in Australian culture. Not surprisingly, this situation indicates that it is normal for an Australian computer forensic expert to show his or her advantages and uniqueness. He or she is not trying to damage the accordance within a group. In short, a Taiwanese computer forensic expert should realize that this behaviour is only a part of Australian culture, and does not have other meanings.

If a Taiwanese computer forensic expert works as a manger or a member of the cross-cultural team, he or she should realize that Australian culture does not focus on the value of the regulation. Australian culture is willing to accept different opinions. This situation infers that creative behaviours and thoughts may be produced unexpectedly, and incredible outcomes may be generated by these innovative behaviours and thoughts. In short, a Taiwanese computer forensic expert should realize that an Australian

computer forensic expert does not completely follow predefined rules due to his or her cultural background rather than the disrespect of the leadership.

If a Taiwanese computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that Australian computer forensic experts emphasize outlines rather than details of the project. In Australian culture, there is no concept of only one correct answer to a question, and the rules of this nature are not valued. On the other hand, Australian culture is willing to accept different opinions, and seeks innovative thoughts and solutions. This infers that Australian culture emphasizes the value of creativity. Thus, details of a project are not always necessary for Australian computer forensic experts. In short, a Taiwanese computer forensic expert should provide enough space for Australian computer forensic experts to be creative in order not to restrict any possible solutions.

If a Taiwanese computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that Australian culture emphasizes the value of personal performance. In addition, Australian culture emphasizes the performance of an individual. Performance is a very important factor to evaluate an individual. This indicates that a Taiwanese manager may find out it is hard for an Australian computer forensic expert to work as a team with other computer forensic workers since Australian culture focuses on individualism. In short, a Taiwanese manager has to understand the nature of Australian culture when he or she allocates tasks.

If a Taiwanese computer forensic expert works as a manager or a member of a cross-cultural team, he or she should realize that the concept of hierarchy is not respected in Australian culture. In Australian culture, people have equal rights since hierarchy only indicates differences of roles. Not surprisingly, a Taiwanese manager may feel offended by some behaviours or verbalities of Australian computer forensic experts. In fact, it is not their intention to challenge the leadership of the manager, but this is only the characteristics of their culture. In short, a Taiwanese manager should understand the different behaviours of Australian computer forensic experts.

7.5.3 Suggestions for Australian and Taiwanese Computer Forensic Experts by Dimensions

In Current Situation Dimension, Australian computer forensic experts should realize that the development of computer forensics in Taiwan is not as progressive as in Australia. This is mainly because the Taiwanese government understood the importance of computer forensic issues, and studied these issues later than the Australian government. Not surprisingly, many rules and regulations are developing in Taiwan at this moment. For example, the SOPs of a computer forensic investigation is an ongoing project. In short, Australian computer forensic experts must remember that what is basic in Australia may be not so well-known or well-accepted in Taiwan.

In addition, Taiwanese computer forensic experts should realize that the current development of computer forensics in Australia is indeed more advanced than in Taiwan. However, this does not mean that their rules or methods can be directly and completely used in Taiwan without any modification. Two essential standpoints should be understood. The first perspective is that the computer forensic applications may be developed in more details in Australian, but they are still not perfect. There are is much work needed to be done to improve the current computer forensic applications in Australia. The second perspective is that the methods accepted in Australia may be not suitable for the conditions in Taiwan. In summary, Taiwanese computer forensic experts must remember that learning from Australian methods is a good idea but this transfer of idea should be conducted carefully.

In the Policy and Organization Dimension, Australian computer forensic experts should realize that the Taiwanese policies associated with computer forensic issues are not well-developed and there are only federal-level computer forensic organizations in Taiwan at present. This situation indicates that it is the beginning stage of the development of computer forensics. Thus, Australian computer forensic experts must realize that Taiwan needs time to develop its own suitable policies and to establish appropriate organizations.

In addition, Taiwanese computer forensic experts should realize that the policies and organizations are developed more systematically in Australia. The existence of Cybercrime/Computer Crime Legislation 2001 is a good example for this statement. In addition, computer forensic organizations are built hierarchically. The federal-level and

state-level computer forensic organizations have different responsibilities and jurisdictions. In summary, Taiwanese computer forensic experts should learn systematic development attitudes and processes from the Australian culture.

In the Education Dimension, Australian computer forensic experts should realize that the educational programs for developing computer forensic investigators are not well-developed. In addition, the major training method is sending computer forensic investigators overseas for advanced courses. Thus, Australian computer forensic experts must realize that the educational and training programs within the field of computer forensic field are a good start point for forming the cooperation between Australia and Taiwan.

In addition, Taiwanese computer forensic experts should realize that professional experience and expertise is respected in Australian culture. A PhD degree may mean nothing in Australian culture. The educational qualification of an Australian computer forensic investigator may be equated to his or her ability. In short, a Taiwanese computer forensic expert should not disrespect an Australian computer forensic investigator if he or she does not have an excellent academic background. This also indicates that Taiwanese computer forensic experts must realize that Australian culture focuses on the experience, expertise, and ability of an individual.

In the Law Dimension, Australian computer forensic experts should realize that the legislation is not well-developed in Taiwan. Not surprisingly, this condition infers that the digital evidence does not have a high weight in a court in Taiwan. This situation actually reveals that computer forensics is a relatively young subject in Taiwan. Thus, Australian computer forensic experts must realize that most conditions in Taiwan may be different from those in Australia. For example, digital evidence has a higher probability of being rejected by a court of law in Taiwan.

In addition, Taiwanese computer forensic experts should realize that the development of legislation is relatively satisfactorily in Australia. For example, the existence of Cybercrime/Computer Crime Legislation 2001 is a good proof for this statement. This situation shows that the computer forensic issues are dealt with more systematically in Australia. In short, this constructive attitude could be adopted by Taiwanese culture.

In the Personal Preferences and Skills Dimension, Australian computer forensic experts should realize that people in Taiwan are used to protecting themselves from others. This means that Australian computer forensic experts may find it very hard to make friends with people in Taiwan. However, this situation is just the nature of Taiwanese culture, and does not have any other meanings. In addition, Taiwanese culture shows different attitude toward professional skills. For example, Taiwanese culture usually focuses more on the certifications than the ability of an individual. In short, Australian computer forensic experts should have an open-mindedness to these cultural differences, and not think that the people in Taiwan reject them.

In addition, Taiwanese computer forensic experts should realize that Australian culture is relaxed and comfortable. In general, people in Australian are friendly and open. This means that Taiwanese computer forensic experts may find it very easy to make develop collegial relationships with people in Australia. However, the standpoint should be realized is that people in Australia treat things independently. Interpersonal relationship does not change basic values. Moreover, Australian culture concentrates on professional experience, expertise, and ability of an individual when discussing skills of an individual.

7.6 Future Works

This thesis not only shows the relationship between different the Australian and Taiwanese cultures in the field of computer forensics, but also provides suggestions, associated with the cross-cultural cooperation, for Australian and Taiwanese computer forensic workers. By understanding these suggestions, this thesis hopes to assist the future cooperation between Australia and Taiwan in quantity and quality. However, there are a number of areas in which this work can be expanded, in both context, field and the cultures analyzed.

The subsequent works of this research can be explained and classified from the following two standpoints. This first type of the subsequent works is that other countries can be used as research targets to further confirm the relationship between culture and computer forensic applications. For example, expanding this work to mainland China (the country with most population in Chinese culture), or the United States of America (the country with the leading research results of computer forensics in Western culture)

would be two countries that is would be beneficial to expand this research to. Whilst in many ways, the cultural characteristics in mainland China expected to be similar to the cultural characteristics in Taiwan in many ways, and an analysis of the United States of America is expected to have similarities with the Australian cultural outcomes of this research. However, there will be differences unique to each culture that would require data collection to discover. However, the outcomes of expanding this research to different countries will make the outcomes more flexible – given the standard analysis, all countries could be examined and compared. Adding analysis of two more countries would allow the comparison from any culture to any other. For example, adding a cultural analysis of China and the United States of America would allow a comparison between China and Taiwan, or the United States, China and Australia. This type of research is interesting since it is able to collect useful data from computer forensic experts with other nationalities.

The second type of potential subsequent work that is an outcome of this research is that the context of this work can be expanded to other forensic sciences such as fingerprint examination and DNA testing. This is true as computer forensics can be considered a subject within the field of forensic science. Thus, it is reasonable to infer that culture must have certain impacts on the applications of forensic science. This type of research is an interesting topic for the future work of this thesis. In summary, this type of research is able to improve the trustworthiness of the research problem of this thesis, and shows that culture is a worthwhile factor even for the forensic science.

7.7 Conclusion to Research

This research sought to determine whether culture impacts computer forensic processes and applications. To do this, the research collected three sources of data (literature, Delphi survey instrument and case study interview) and compared the Australian and Taiwanese cultures in five different dimensions. These dimensions were; Current Situation, Policy and Organization, Education, Law, and Personal Preferences and Skills.

The outcomes of this work showed that culture does indeed impact the field of computer forensics in all of the listed dimensions, both for each country independently and then comparatively. This work was able to determine how these cultures differ, the

chief characteristics of each culture, and also go further and discuss how inter-culture communication and team-sharing would need to consider each cultural source. In this it was successful, and one of the major asset outcomes of this work is a series of suggestions for inter-cultural computer forensic work between Australia and Taiwan – the first of its kind.

8 Reference

Ahmad, A. (2002). The Forensic Chain of Evidence Model Improving the Process of Evidence Collection in Incident Handling Procedures. Proceedings of the 6th Pacific Asia Conference on Information Systems.

Alavi, M., and Carlson, P. (1992). A Review of MIS Research and Disciplinary Development, Journal of Management Information Systems, pp. 45-62.

Albinski, H. S. (2001). Cultural Reflections. Australian Journal of International Affairs, pp. 275-285.

Ali, A. K. (2005). Using the Delphi Technique to Search for Empirical Measures of Local Planning Agency Power. The Qualitative Report, pp. 718-744.

Allen, W. H. (2005). Computer Forensics. IEEE Security and Privacy Magazine, pp. 59-62.

Amaratunga, D., and Baldry, D. (2001). Case Study Methodology as a means of Theory Building: Performance Measurement in Facilities Management Organisations. Work study, pp.95-105.

American National Science Teachers Association (1998). American National Science Teachers Association. Available at: http://www.nsta.org/.

Association of Chief Police Officers (2003). Good Practice Guide for Computer based Electronic Evidence. Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Australasian Centre for Computing Research (2003). Seizing Computers and other Electronic Evidence. Available at: http://www.acpr.gov.au/publications2.asp?Report_ID=130

Australasian Centre for Policing Research (2007). Australasian Centre for Policing Research. Available at: http://www.acpr.gov.au/about.asp.

Barbara, J. J. (2005). Digital Evidence Accreditation in the Corporate and Business Environment. Digital Investigation, pp. 137-146.

Bardecki, M. J. (1984). Participants' Response to the Delphi Method: An Attitudinal Perspective. Technological Forecasting and Social Change, pp. 281-292.

Baryamureeba, V. and Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. Digital Forensic Research Workshop 2004.

Bates, J. (1998). Fundamentals of Computer Forensics. Information Security Technical Report, pp. 75-78.

Beckett, J., and Slay, J. (2007). Digital Forensics: Validation and Verification in a Dynamic Work Environment. Proceedings of the 40th Hawaii International Conference on System Sciences.

Benarie, M. (1988). Delphi and Delphi like Approaches with Special Regard to Environmental Standard Setting. Technological Forecasting and Social Change, pp. 149-158.

Biggs, J. (1996). Western Misperceptions of the Confucian-Heritage Learning Culture. The Chinese Learner: Cultural, Psychological and Contextual Influences (Edited by Watkins D. A., and Biggs, J.).

Boyd, C., and Forster, P. (2004). Time and Date Issues in Forensic Computing - A Case Study. Digital Investigation, pp. 18-23.

Brilis, G. M., Waasbergen, R. J. V., Stokely, P. M., and Gerlach, C. L. (2001). Remote Sensing Tools Assist in Environmental Forensics: Part II—Digital Tools. Environmental Forensics, pp. 223-229.

Buchholz, F., and Spafford, E. (2004). On the Role of File System Metadata in Digital Forensics. Digital Investigation, pp. 298-309.

Buchholz, F., and Falk, C. (2005). Design and Implementation of Zeitline: A Forensic Timeline Editor. Available at: dfrws.org/2005/proceedings/buchholz_zeitline.pdf

Buzzell, R. D. (1968). Can you standardize multinational marketing?. Harvard Business Review, pp. 102-113.

Cagilitay, K. (1999). Culture and its Effects on Human-Computer-Interaction. Ed-Media 99.

Campbell, D. T. (1975). Degrees of Freedom and the Case Study. Comparative Political Studies, 99.178-193.

Carrier, B., and Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence.

Carter, G. B., 1995, Australian Legal System. Blackstone Press Pty Ltd.

Casey, E. (2000). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet with Cdrom. Academic Press.

Casey, E. (2002). Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence.

Castigline, A., Santis, A. D., and Soriente, C. (2007). Taking Advantages of a Disadvantage: Digital Forensics and Steganography using Document Metadata. Journal of Systems and Software, pp. 750-764.

Cetron, M. J. (1969). Technological Forecasting. New York: Fordon and Breach.

Chaski, C. E. (2005). Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations. International Journal of Digital Evidence.

Christopher, C., and Hidgekiss, S. C. (2006). Expert Evidence in Competition Litigation. Trade Practices Law Journal.

Chua, W. F. (1986). Radical Developments in Accounting Thought. The Accounting Review, pp. 601-632.

Civie, V., and Civie, R. (1998). Future Technologies from Trends in Computer Forensic Science. IEEE Information Technology Conference, pp.105-108.

Clarke, R. (2000). Appropriate Research Methods for Electronic Commerce. Available at: http://www.anu.edu.au/people/Roger.Clarke/EC/ResMeth.html

Clayton, M. J. (1997). Delphi: A Technique to Harness Expert Opinion for Critical Decision-Making Tasks in Education, Educational Psychology: An International Journal of Experimental Educational Psychology.

Coates, J. F. (1975). In Defense of Delphi. Technological Forecasting and Social Change, pp. 193-194.

Cobern, W. W. (1991). World View Theory and Science Education Research. NARST Monograph NO. 3. Manhattan, KS: National Association for Research in Science Teaching.

Cobern, W. W., and Loving, C. C. (1998). Defining "Science" in a Multicultural World: Implications for Science Education. Annual Meeting and Conference of the NARST.

Cobern, W. W., Gibson, A. T., and Underwood, S. A.(1999). Conceptualizations of Nature: An Interpretive Study of 16 ninth Graders' Everyday Thinking. *Journal of Research in Science Teaching*, pp. 541-564.

Command and Control Research Program Office of the Assistant Secretary of Defensefor Command, Control, Communications and Intelligence (CCRP). (2001). Sensemaking Symposium Final Report. Evidence Based Research Inc. Available at: http://www.dodccrp.org/

Cooper, P. (2005). Speciation in the Computing Sciences: Digital Forensics as an Emerging Academic Discipline. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development.

Creswell, J. W. (1998). Qualitative Inquiry and Research Design. SAGE Publication.

Criminal Investigation Bureau (2007). Criminal Investigation Bureau. Available at: http://www.cib.gov.tw/.

Crispino, F. (2007). Nature and Place of Crime Scene Management within Forensic Sciences. Science and Justice.

Cronbach, L. J. (1975). Beyond the two disciplines of scientific psychology. American Psychologist, pp. 116-127.

Custer, R. L., Scarcella, J. A., and Stewart, B. R. (1999). The Modified Delphi Technique – A Rotational Modification. Journal of Vocational and Technical Education. Available at: http://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html

DAAN Police District of Taipei City Police Department (2007). DAAN Police District of Taipei City Police Department. Available at: http://tapp.tcpd.gov.tw.

Dafoulas, G., and Macaulay, L. (2001). Investigating Cultural Differences in Software Teams. Electronic Journal on Information Systems in Developing Countries, pp. 1-14.

Dajani, J., Sincoff, M., and Talley, W. (1979). Stability and Agreement Criteria for the Termination of Delphi Studies. Technological Forecasting and Social Change, pp. 83-90.

Dalkey, N. C. (1969). The Delphi Method: An Experimental Study of Group Opinion. Available at: http://www.rand.org/pubs/research_memoranda/2005/RM5888.pdf

Dalkey, N. C., and Helmer, O. (1963). An Experimental Application of the Delphi Method to the Use of Experts. Management Science, pp. 458-467.

Davies, G. L. (2006). Civil Justice Reform: Some Common Problems, Some Possible Solutions. Journal of Judicial Administration.

Davies, D., and Dodd, J. (2002). Qualitative Research and the Question of Rigor. Qualitative Health Research, pp. 279-289.

Delbecq, A. L., Van de Ven, A. H., and Gustafson, D. H. (1986). Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes. WI: Green Briar Press.

De Loe, R. C. (1995). Exploring complex Policy Questions using the Policy Delphi: A Multi-Round, Interactive Survey Method. Applied Geography, pp. 53-68.

Department of Border Police (2007). Department of Border Police. Available at: http://cpuweb2.cpu.edu.tw/border/index(new).html.

Department of Fire Science (2007). Department of Fire Science. Available at: http://cpuweb2.cpu.edu.tw/fire/index1024.htm.

Department of Forensic Science (2007). Department of Forensic Science. Available at: http://cpuweb2.cpu.edu.tw/forensic/.

Department of Information Management (2007). Department of Information Management. Available at: http://www.im.cpu.edu.tw/.

Department of Maritime Police (2007). Department of Maritime Police. Available at: http://cpuweb2.cpu.edu.tw/maritime/.

Department of Public Security (2007). Department of Public Security. Available at: http://cpuweb2.cpu.edu.tw/security/.

Denning, D., and Baugh, W. (1997). Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism. The National Strategy Information Center's US Working Group on Organized Crime (WGOC).

Denzin, H. (1984). The Research Act. Englewood Cliffs, NJ: Prentice Hall.

Denzin, N. K., and Lincoln, Y. S. (1994). Handbook of Qualitative Research. Thousand Oaks, CA: SAGE.

De Vaus, D. (2001). Research Design in Social Research. SAGE Publications.

Dixon, P. D. (2005). An Overview of Computer forensics. IEEE Potentials, pp. 7-10.

Duboff, R., and Spaeth, J. (2000). Marker Research Matters: Tools and Techniques for Aligning Your Business. New York: John Wiley & Sons.

Duren, M., and Hosmer, C. (2002). Can Digital Evidence endure the Test of Time? Proceedings of the Second Digital Forensic Research Workshop.

Easterby-Smith, M. (1991). Management Research: An Introduction, Sage Publications, London.

Eisner, E. W. (1991). The enlightened eye: Qualitative inquiry and the enhancement of educational practice. New York, NY: Macmillan Publishing Company.

Erbacher, R. F., Endicott-Popovsky, B., Frincke, D. A. (2007). Challenge Paper: Validation of Forensic Techniques for Criminal Prosecution. Second International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 150-154.

Erez, M., and Earley, P. C. (1993). Culture, Self-Identity and Work. Oxford University Press.

Ezzy, D. (2002). Qualitative Analysis : Practice and Innovation. Routledge.

Feagin, J., Orum, A., and Sjoberg, G. (1991). A Case for Case Study. NC: University of North Carolina Press.

Federal Bureau of Investigation (2003). Crime-Scene Search. Available at: http://www.fbi.gov/hq/lab/handbook/intro16.htm

Finkelstein, A., and Fuks, H. (1989). Multi-party Specification. The fifth Conference on Software Specification and Design.

Fitch, K., Berstein, S. J., Aguilar, M. D., Burnard, B., Lacalle, J. R., and Lazaro, P. (2001). The Rand/UCLA Appropriateness Method User's Manual. CA: RAND

Ford, D. (1975). Shang Inquiry as an alternative to Delphi: Some Experimental Findings. Technological Forecasting and Social Change, pp. 139-146.

Forte, D. (2003). Principles of Digital Evidence Collection. Network Security, pp. 6-7.

Francia, G. A. (2006). Digital Forensics Laboratory Projects. Journal of computing Sciences in Colleges.

Freeh, L. J. (1997). Impact of Encryption on Law Enforcement and Public Safety. Trends in Organized Crime.

Geertz, C. (1973). The Interpretation of Cultures. New York: Basic Books, Inc.

Ghosh, A. (2004). Guidelines for the Management of IT Evidence. Incident Response and Forensics Workshop APEC-Tel 29. Available at: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Gladyshev, P., and Patel, A. (2005). Formalising Event Time Bounding in Digital Investigations. International Journal of Digital Evidence.

Glesne, C., and Peshkin, A. (1992). Becoming qualitative researchers: An introduction. White Plains, NY: Longman.

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. The Qualitative Report, pp. 597-607.

Goldsworthy, D. (2005). Australian External Policy and the End of Britain’s Empire. Australian Journal of Politics and History, pp. 17-29.

Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., and Stein, M. (2005).Computer Forensics Programs in Higher Education: A Preliminary Study. Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education, pp. 147-151.

Green, H., Hunter, C., and Moore, B. (1990). Assessing the Environmental Impact of Tourism Development: Use of the Delphi Technique. Tourism Management, pp. 111-120.

Greenfield, P. M. (1997). Culture as Process: Empirical Methods for Cultural Psychology. In J. W. Berry, Y. Poortinga, & J. Pandey (Eds.), Handbook of Cross-Cultural Psychology: Vol. 1: Theory and Method. (pp. 301- 346). Boston: Allyn & Bacon.

Gupta, U., and Clarke, R. (1996). Theory and Applications of the Delphi Technique: A Bibliography (1975-1994). Technological Forecasting and Social Change, pp. 185-211.

Haifeng, L. (2006). Rehabilitation of the Imperial Examination System. Frontiers of Education in China.

He, Z. W., Bu, J.Z., Tang, Y. Y., and Sun, K. T. (1991). An Intellectual History of China. Beijing: Foreign Languages Press.

Heilbronn, G. (2002). Introducing the Law. CCH Australia Limited.

Herath, A., Herath, S., Samarasinghe, P., Herath, J. (2005). Computer Forensics, Information Security and Law: A Case Study. First International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 135-141.

Hirschheim, R. A. (1985). Information systems epistemology: An historical perspective. In E. Mumford, R. Hirschheim, G. Fitzgerald & T. Wood-Harper (Eds.), *Research Methods in Information Systems* (pp. 13-35). North-Holland.

Ho, D. Y. F. (1991). Cognitive Socialization in Confucian Heritage Cultures. Workshop on Continuities and Discontinuities in the Cognitive Socialization of Minority Children, US Department of Health and Human Services.

Hofstede, G. (1980). Motivation, Leadership, and Organization: Do American Theories Apply Abroad?. Organizational Dynamics, pp. 42-63.

Hofstede, G. (1986). Culture Differences in Teaching and Learning. International Journal of Intercultural Relations, pp.301-320.

Hofstede, G. (1989). Organising for Cultural Diversity. European Management Journal, pp. 390-397.

Hofstede, G. (1993). Cultural Constraints in Management Theories. Academy of Management Executive, pp. 81-94.

Hofstede, G. (1994). The Business of International Business is Culture. International Business Review, pp. 1-14.

Hofstede, G. (2007). Hofstede's Scores. Available at: http://www.geert-hofstede.com/hofstede_dimensions.php

Hofstede, G., and Bond, M. H. (1988). The Confucius Connection: From Cultural Roots to Economic Growth. Organizational Dynamics, pp. 5-21.

Hojring, K. (2002). The Right to Roam the Countryside – Law and Reality Concerning Public Access to the Landscape in Denmark. Landscape and Urban Planning, pp. 29-41.

Holton, G. (1993). Science and Anti-Science. Cambridge, MA: Harvard University Press.

Hong. P.Z. (1991). A Thorny Journey - A Study of the Acculturation Process of Some Chinese ELICOS Students in Brisbane, Australia. Griffith University: Brisbane, Australia.

Horne, D. (1964). The Lucky Country. Ringwood, Vic. : Penguin.

Hosmer, C. (2002). Proving the Integrity of Digital Evidence with Time. International Journal of Digital Evidence.

Hwang, C. L., and Lin M. J. (1987). Group Decision Making under Multiple Criteria Methodsand Application. Berlin, Germany: Springer-Verlag, pp. 169-174.

IThome online (2006). 調查局成立第一座國家級資安鑑識實驗室. Available at: http://www.ithome.com.tw/itadm/article.php?c=41099

Jegede, O. J. (1994). African Cultural Perspectives and the Teaching of Science. In STS Education: International Perspectives on Reform, Solomon, J. and Aikenhead, G. (ed.), New York: Teachers College Press.

Jingpan, C. (1990). Confucius as A Teacher-Philosophy of Confucius with Special Reference to its Educational Implications. Foreign Languages Press.

Jones, N. (2004). Training and Accreditation – Who are the Experts? Digital Investigation, pp. 189-194.

Jones, A. and Meyler, C. (2004). What Evidence is Left after Disk Cleaners? Digital Investigation.

Joppe, M. (2000). The Research Process. Available at: http://www.ryerson.ca/~mjoppe/rp.htm

Kearney, M. (1984). World View. Novato, CA: Chandler & Sharp.

Kedia, B. L., and Bhagat, R. S. (1988). Cultural Constraints on Transfer of Technology Across Nations: Implications for Research in International and Comparative management. Academy of Management Review, pp. 559–571.

Kendall, J. (1977). Variations of Delphi. Technological Forecasting and Social Change, pp. 75-85.

Kenneally, E. E. (2004). Digital Logs – Proof Matters. Digital Investigation.

Kenneally, E. E., and Brown, C. L. T. (2005). Risk Sensitive Digital Evidence Collection. Digital Investigation, pp. 101-119.

Kilbourn, B. (1984). World Views and Science Teaching. In Munby, H., Orpwood, G., and Russel, T. (eds.), Seeing Curriculum in a New Light. Lanham, MD: University Press of America.

King, A. Y. C., and Bond, M. H. (1985). The Confucian Paradigm of Man: a Sociological View, in Tseng, W. and Wu, D. (Eds). Chinese Culture and Mental Health, pp. 29-45.

Kirk, J., and Miller, M. L. (1986). Reliability and Validity in Qualitative Research. Beverly Hills: Sage Publications.

Kruse, W. G., and Heiser, J. G. (2002). Computer Forensics: Incident Response Essentials. Addison-Wesley.

Landwehr, C. E. (2001). Computer Security. Journal of Information Security, pp. 3-13.

Lee, S., Kim, H., Lee, S., and Lim, J. (2005). Digital Evidence Collection Process in Integrity and Memory Information Gathering. Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 236-247.

Legge, J. (1893). The Analects of Confucius. Clarendon Press.

Levitt, N., and Gross, P. R. (1994). The Perils of Democratizing Science. The Chronicle of Hifher Education.

Li, X., and Seberry, J. (2003). Forensic Computing. In 4th International Conference on Cryptology.

Lin, I-L., Yang, H.-C., Gu, G.-L., and Lin, A.-C. (2003a). A Study of Information and Communication Security Forensic Technology Capability in Taiwan. IEEE 37th

Annual 2003 International Carnahan Conference on security Technology, pp. 386-393.

Lin, I-L., Lan, T.-S., and Wu, J.-C. (2003b). A Research of Information and Communication Security Forensic Mechanism in Taiwan. IEEE 37th Annual 2003 International Carnahan Conference on security Technology, pp. 23-29.

Lin, A.-C., Lin, I-L., Lan, T.-H., and Wu, T.-C. (2005). "Establishment of the Standard Operating Procedure (SOP) for Gathering Digital Evidence", Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 56-65.

Lincoln, Y. S., and Guba, E. G. (1985). Naturalistic Inquiry. Beverly Hills, CA: Sage.

Linstone, H. A., and Turoff, M. (1975). The Delphi Method: Techniques and Applications, Addison-Wesley Publishing Company.

Linstone, H. A., and Turoff, M. (2002). The Delphi Method: Techniques and Applications. Available at: http://is.njit.edu/pubs/delphibook/.

Liophanich, C. (2005a). An Automatic E-Evidence Archival System. 3rd IEEE International Conference on Industrial Informatics, pp. 209-214.

Liophanich, C. (2005b). Automatic E-Evidence Generation System and Duplicate Reduction. IEEE International Conference on Services Computing, pp. 167-174.

Liu, J. (2006). Developing an Innovative Baccalaureate Program in Computer Forensics. 36th Annual Frontiers in Education Conference, pp. 1-6.

Luoma, V. M. (2006). Computer Forensics and Electronic Discovery: The New Management Challenge. Computer & Security, pp. 91-96.

Marie, C. H. (1997). Choosing Qualitative Research: A Primer for Technology Education Researchers. Journal of Technology Education.

Martin, A. G., and Frick, M. J. (1998). The Delphi Technique: An Informal History of its Use in Agricultural Education Research since 1984. Journal of Agricultural Education, pp. 73-79.

Mathison, S. (1988). Why Triangulate? Educational Researcher, pp. 13-17.

McKemmish, R., (1999). What is Forensic Computing?, Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice.

McLean, D. (2006). From British Colony to American Satellite? Australia and the USA during the Cold War. Australian Journal of Politics and History, pp. 64-79.

Merchant, C. (1989). The Death of Nature: Women, Ecology, and the Scientific Revolution. San Francisco, CA: Harper & Row.

Mercuri, R. T. (2005). Challenges in Forensic Computing. Communications of ACM.

Meyers, M., and Rogers, M. (2004). Computer Forensics: The Need for Standardization and Certification. International Journal of Digital Evidence.

Miller, M. M. (1993). Enhancing Regional analysis with the Delphi Method. Review of Regional Studies, pp. 191-212.

Mingers, J. (2001) Combining IS Research Methods: Towards a Pluralist Methodology, Information Systems Research, pp. 240-259.

Ministry of the Interior (2003). Investigating Principles for Police Force. Available at: http://pan.jolios.com/date/WORD/W005/w9-001.htm

Mocas, S. (2004). Building Theoretical Underpinnings for Digital Forensics Research. Digital Investigation, pp. 61-68.

Mohay, G., Anderson, A, Collie, B, McKemmish, R., and de Vel, O. (2003). Computer and Intrusion Forensics, Artech House, Norwood, MA, USA.

Mohay, G. (2005). Technical Challenges and Directions for Digital Forensics. First Internatioinal Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 155-161.

Myers, M. D. (1997). Qualitative Research in Information Systems. MISQ Discovery.

National Institute of Forensic Science (2007). National Institute of Forensic Science. Available at: http://www.nifs.com.au/.

National Institute of Justice (2000). Crime Scene Investigation: A Guide for Law Enforcement, Available at: http://www.ncjrs.gov/pdffiles1/nij/178280.pdf

National Institute of Justice (2001a). Searching and Seizing Computers and Related Electronic Evidence Issues. Available at: http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

National Institute of Justice (2001b). Electronic Crime Scene Investigation – A Guide for First Responders, Available at: http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

National Institute of Justice (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Available at: http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

National Institute of Justice (2007). Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, Available at: http://www.ncjrs.gov/pdffiles1/nij/211314.pdf

National Kaohsiung First University of Science and Technology (2007). National Kaohsiung First University of Science and Technology. Available at: http://www.nkfust.edu.tw/english/.

National Police Agency, Ministry of the Interior (2007). About Chief. Available at: http://www.npa.gov.tw/NPAGip/wSite/ct?xItem=31428&ctNode=11686

Nelson, C., Treichler, P. A., and Grossberg, L. (1992). Cultural Studies: An Introduction. Cultural Studies, pp. 1-16.

Newsted, P. R., Chin, W., Ngwenyama, O., and Lee, A. (1997) Resolved: Surveys have Outlived their Usefulness in IS Research. Panel presented at the 1996 International Conference on Information Systems, Cleveland, Ohio.

Newsted, P., Huff, S., Munro, M., Schwarz, A. (1998). A Tutorial on Survey Instruments. MISQ Discovery.

Ogawa, M. (1998). A Cultural History of Science Education in Japan: An Epic Description. In W. W. Cobern (Ed.), Socio-Cultural Perspectives on Science Education: An International Dialogue. Dordrecht, The Netherlands: Kluwer Academic Publishers.

Ogunniyi, M. B. (1988). Adapting Western Science to Traditional African Culture. International journal of Science Education.

Okoli, C., and Pawlowski, S. D. (2004). The Delphi Method as A Research Tool: An Example, Design Considerations and Applications. Information & Management, pp. 15-29.

Orlikowski, W. J., and Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. Information Systems Research, pp. 1-28.

Quaile, K., and Fowles, J. (1975). The Methodological Worth of the Delphi Forecasting Technique. Technological Forecasting and Social Change, pp. 179-192.

Palmer, G. (2001). A Road Map for Digital Forensic Research. The First Digital Forensic Research Workshop.

Pan, L., and Batten, L. M. (2005). Reproducibility of Digital Evidence in Forensic Investigations. 2005 Digital Forensic Research Workshop.

Parente, F. J., Anderson, J. K., Myers P., and O' Brien, T. (1984). An Examination of Factors contributing to Delphi Accuracy. Journal of Forecasting, pp. 173-182.

Patel, A., and Ciardhuain, S. O. (2000). The Impacts of Forensic Computing on Telecommunications. IEEE Communications Magazine, pp. 64-67.

Patton, M. Q. (1990). Qualitative Evaluation and Research Methods (2nd ed.). Newbury Park, CA: Sage Publications, Inc.

Patton, M. Q. (2001). Qualitative Research & Evaluation Methods (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Patzakis, J. (2003). New Accounting Reform Laws Push for Technology-Based Document Retention Practices. International Journal of Digital Evidence.

Platt, R. (2006). Crime Scene: The Ultimate Guide to Forensic Science. DK ADULT.

Poh-Ling, T. (1997). Asian Legal System. Butterworths.

Pollitt, M. M. (1995a). Computer Forensics: An Approach to Evidence in Cyberspace. Proceedings of the National Information Systems Security Conference, pp. 487-491.

Pollitt, M. M. (1995b). Principles, Practices, and Procedures: An Approach to Standards in Computer Forensics. Second International Conference on computer Evidence, pp. 10-15.

Porada, V., and Straus, J. (2007). Digital Evidence in Criminalistic Theory of Traces. Forensic Science International, pp. s37-s38.

Proper, H., Wideen, M. F., and Ivany, G. (1988). World View Projected by Science Teachers: A Study of Classroom Dialogue. Science Education, pp. 542-560.

Radio Taiwan International (2006). 「資安鑑識實驗室」掛牌　電腦犯罪無所遁形. Available at: http://www.rti.org.tw/News/NewsContentHome.aspx?NewsID=57516&t=1.

Ragin, C. C. (1989) The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies, Publisher: University of California Press (March 28, 1989)

Ramsland, K. M. (2001). Forensic Science of CSI. Berkley Trade.

Rathod, M. M., and Miranda, S. M. (1999). Teleworking and Psychological Distance: The Mediating Effects of Culture and Technology in Four Countries. ACM SIGCPR'99, New Orleans, USA.

Reeves, G., and Jauch, L. R. (1978). Curriculum development through Delphi. Research in Higher Education, pp. 157-168.

Reith, M., Carr, C., and Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, pp. 40-51.

Remenyi, D., Williams, B., Money, A., and Swartz, E. (1998). Doing Research in Business and Management. Sage Publications, London.

Richard III, G. G., Roussev, V., and Marziale, L. (2007). Forensic Discovery Auditing of Digital Evidence Containers. Digital Investigation, pp. 88-97.

Riggs, W. (1983). The Delphi Technique: An Experimental Evaluation. Technological Forecasting and Social Change, pp. 89-94.

Robertson, B., and Vignaux, G. A. (1995). Interpreting Evidence: Evaluating Forensic Science in the Courtroom. New York: J. Wiley.

Rowe, G., Wright, G., and Bolger, F. (1991). Delphi: A Reevaluation of research and Theory. Technological Forecasting and Social Change, pp. 235-251.

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence.

Saaty, T. L. (1994). Decision Making in Economic, Political, Social and Technological Environments: The Analytic Hierarchy Process. University of Pittsburgh: RWS Publications.

Sackman, H. (1974). Delphi Assessment: Expert opinion, Forecasting and Group Processs. Santa monica, California: The Rand Corporation.

Saferstein, R. (2001). Criminalistics: An Introduction to Forensic Science. Prentice Hall.

Schatz, B., Mohay, G., and Clark, A. (2006). A Correlation Method for Establishing Provenance of Timestamps in Digital Evidence. Digital Investigation, pp. 98-107.

Schramm, W. (1971). Notes on case studies of instructional media projects. Working paper for the Academy for Educational Development, Washington, DC.

Scientific Working Group on Digital Evidence (1999). Digital Evidence: Standards and Principles**.** Forensic Science Communications.

Scientific Working Group on Digital Evidence (2004a). SWGDE Recommended Guidelines for Validation Testing**.** Available at: http://68.156.151.124/documents/swgde2004/SWGDE%20Validation%20Guidelines%20_July%202004_.pdf

Scientific Working Group on Digital Evidence (2004b). Recommended Guidelines for Developing Standard Operating Procedures. Available at: http://68.156.151.124/documents/swgde2004/SWGDE%20Validation%20Guidelines%20_July%202004_.pdf

Scientific Working Group on Digital Evidence (2005)._Best Practices for Computer Forensics. Available at: http://68.156.151.124/documents/swgde2005/SWGDE%20Best%20Practices%20_Rev%20Sept%202004_.pdf

Scientific Working Group on Digital Evidence (2006). Best Practices for Computer Forensics. Available at: http://68.156.151.124/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf

Seale, C. (1999). Quality in Qualitative Research. Qualitative Inquiry, pp. 465-478.

Shore, B., and Cross, B. J. (2005). Exploring the role of national culture in the management of large-scale international science projects. International Journal of Project Management, pp. 55-64.

Shore, B., Venkatachalam, A.R. (1995). The Role of Culture in System Analysis and Design. Journal of Global Information Management, Vol. 3 No.3, pp.5-14.

Siegfried, J., Siedsma, C., Countryman, B.-J., and Hosmer, C. D. (2004). Examining the Encryption Threat. International Journal of Digital Evidence.

Slay, J. (1998). Using the WWW to Create an Effective Cross-Cultural Learning Environment. Hong Kong Web Symposium 98.

Slay, J. (2000a). Implementing Modern Approaches to Teaching Computer Science: A Life Long Learning Perspective. 16th World Computer Congress, Beijing, August 21-25.

Slay, J. (2000b). Culture and Conceptualisations of Nature: An Interpretive Analysis of Australian and Chinese perspectives. Science and Mathematics Education Centre, Curtin University of Technology.

Slay, J. (2001). Culture and Sensemaking in Information Warfare. The 2nd Australian Information Warfare and Security Conference.

Slay, J. (2002). A Cultural Framework for the Interoperability of C2 systems. Journal of Information Warfare.

Slay, J., and Kearney, D. (2000). An Australian Perspective on the Role of the WWW within Chinese Tertiary computer Science Education. The Asia Pacific Web Conference.

Slay, J., and Burke, M. M. (2001). A World View Analysis of the Effect of Culture within C2. The 6th International Command and Control Research and Technology Conference.

Slay, J., Darzanos, K., Quirchmayr, G., and Koronios, A. (2003). Towards a Mature Understanding of 'Culture' in Information Systems Security Research. IFIP Joint WG 8.2 + 9.4 Conference, Athens University of Economics & Business, Greece, pp. 15-17.

Slay, J., and Quirchmayr, G. (2004). A Formal Model for the Relationship between Culture and Trust within IS Security Management. The Second Australian Information Security Management Conference.

Slay, J., Hannan, M., Broucek, V., and Turner, P. (2004). Developing Forensic Computing Tools and Techniques within a Holistic Framework: an Australian Approach. In Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop.

Soares, A. M., Farhangmehr, M., and Shoham, A. (2007). Hofstede's Dimensions of Culture in International Marketing Studies. Jurnal of Business Research, pp. 277-284.

Solano-Flores, G., and Nelson-Barber, S. (2001). On the Cultural Validity of Science Assessments. Journal or Research in Science Teaching, pp. 553-573.

Solon, M., and Harper, P. (2004). Preparing Evidence for Court. Digital Investigation, pp. 279-283.

Sommer, P. (2004). The Future for the Policing of Cybercrime. Computer Fraud & Security Bulletin.

Stake, R. (1995). The Art of Case Research. Thousand Oaks, CA: Sage Publications.

Stenbacka, C. (2001). Qualitative Research Requires Quality Concepts of its Own. Management Decision, pp. 551-555.

Stephenson, P. (2003). Modeling of Post-Incident Root Cause Analysis. International Journal of Digital Evidence.

Stevens, M. W. (2004). Unification of Relative Time Frames for Digital Forensics. Digital Investigation, pp. 225-239.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., and Strite, M. (2002). Toward a Theory-Based Measurement of Culture. Journal of Global Information Management, pp. 13-23.

Straub, D., Gefen, D., and Boudreau, M.-C. (2005). Quantitative Research. In Research in Information Systems: A handbook for Researh Supervisors and their Students.

Strauss, A., and Corbin, J. (1990). Basics of qualitative research: Grounded theory procedures and techniques. Newbury Park, CA: Sage Publications, Inc.

Strauss, A., and Corbin, J. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory (2nd ed.). Sage Publications.

Taiwan Computer Emergency Response Team/Coordination Centre (2007). Organization Chart. Available at: http://www.cert.org.tw/about/index.php#architechre

Tamkang University (2007). Tamkang University. Available at: http://foreign.tku.edu.tw/TKUEnglish/.

Tan, J. (2001). Forensic Readiness. CanSecWest Computer Security Conference.

Taylor, S. J., and Bogdan, R. (1998). Introduction to Qualitative Research Methods: A Guidebook and Resource (3rd ed.). John Wiley & Sons, Inc.

Tellis, W. (1997a). Results of a Case Study on Information Technology at a University. The Qualitative Report.

Tellis, W. (1997b). Introduction to Case Study. The Qualitative Report.

Tellis, W. (1997c). Application of a Case Study Methodology. The Qualitative Report.

Tesch, R. (1990). Qualitative Research: Analysis Types and Software Tools. The Falmer Press."

The Chinese Culture Connection (1987). Chinese Values and the Search for Culture-Free Dimensions of Culture. Journal of Cross-Culrural Psychology, pp. 143-164.

Theocharis, T., and Psimopoules, M. (1987). Where Science has Gone Wrong. Nature, pp. 595-598.

Thompson, E. (2005). MD5 Collisions and the Impact on Computer Forensics. Digital Investigation, pp. 36-40.

Turnbull, B. (2007). Wi-Fi as Electronic Evidence: Policy, Process and Tools. School of Computer Information Science, University of South Australia.

Turner, P. (2005). Digital Provenance – Interpretation, Verification, and Corroboration. Digital Investigation, pp. 45-49.

Uhl, N. P. (Editor). (1983). Using Research for Strategic Planning. San Francisco: Jossey-Bass Publishers.

Vogel, D., Davison, R. M., Shroff, R. H., and Qureshi, S. (2001). Sociocultural Learning in Globally Distributed Teams: An Exploratory Study. Proceedings of Informing Science

Volonino, L. (2003). Electronic Evidence and Computer Forensics. Communication of the Association for Information Systems.

Volonino, L., Anzaldua, R., Godwin, J., and Kessler, G. C. (2007). Computer Forensics: Principles and Practices. Pearson / Prentice Hall.

Vygotsky, L. S. (1978). Mind in Society: The Development of Higher Psychological Processes. Cambridge, MA: Harvard University Press.

Waldrip, B. and Taylor, P. C. (1995). Understanding Students' cultural Background: A Prerequisite of Effective Teaching. PNG Journal of Education.

Wang, S. J. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-Based Cyber-Crimes. Computer Standards & Interfaces, pp. 216-223.

Wang, S.-J., and Yang, C.-H. (2005). Gathering Digital Evidence in Response to Information Security Incidents. IEEE International Conference on Intelligence and Security Informatics, Lecture Notes in Computer Science (LNCS).

Wang, X., Yin, Y. L., and Yu, H. (2005). Finding Collisions in the Full SHA-1. Advances in Cryptology – Crypto.

Wang, X., and Yu, H. (2005). How to Break MD5 and other Hash Functions. Advances in Cryptology - Eurocryp, pp. 19-35.

Weil, M. C. (2002). Dynamic Time and Date Stamp Analysis. International Journal of Digital Evidence.

Wertsch, J. V. (1985). Vygotsky and the Social Formation of Mind. Cambridge, MA: Harvard University Press.

Wertsch, J. V., Del Rio, P., and Alvarez, A. (1995). Sociocultural Studies of Mind. New York: Cambridge University Press.

Wilsdon, T., and Slay, J. (2005). Digital Forensics: Exploring Validation, Verification and Certification. In First International Workshop on Systematic Approaches to Digital Forensic Engineering.

Wolfe, H. (2004). Penetrating Encrypted Evidence. Digital Investigation, pp. 102-105.

Woudenberg, F. (1991). An Evaluation of Delphi. Technological Forecasting and Social Change, pp. 131-150.

Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., and Sommer, P. M. (2003). Computer Forensics Education. IEEE Security and Privacy Magazine, pp. 15-23.

Yin, R. K. (1984). Case Study Research: Design and Methods. Beverly Hills, CA: Sage Publications.

Yin, R. K. (1989). Case Study Research: Design and Methods (Rev ed.). Beverly Hills, CA: Sage Publications.

Yin, R. K. (1994). Case Study Research: Design and Methods (2nd ed.). Beverly Hills, CA: Sage Publications.

Zonabend, F. (1992). The Monograph in European Ethnology. Current Sociology, pp. 49-60.

Appendix 1: First Round Questionnaire for Delphi Survey in Australia (English Version)

Section 1: Conditions of Computer Forensics

1. From your point of view, what is your government's perspective on computer forensic issues? Do you think the emphasis they put on it is currently at an appropriate level?
2. What is your opinion on the current developments within computer forensics? Are you satisfied with the current developments of computer forensics? Why?
3. How many years has computer forensics existed as a discipline in your country?
4. Is computer forensics a topical issue in your country?

Section 2: Procedures of Computer Forensics

5. From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?
6. What is your opinion on the importance of SOPs of computer forensic investigations?
7. Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?

Section 3: Characteristics of Computer Forensics

8. Based on your knowledge, what are the main characteristics of digital evidence? (e.g. ***Integrity***)
9. What is your opinion on meta-data of digital evidence from computer forensic perspective?
10. What is your opinion on the trustworthiness of meta-data of digital evidence?
11. How would you describe the relationship between computer security and computer forensics?
12. When performing a computer forensic investigation, is it necessary to understand the background of the investigated person? (How many dogs they have? What cars they drive? Do they have any habit?) or just focus on analysing the digital data? Why?

Section 4: Organization of Computer Forensics

13. In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?
14. In your country, do law enforcement organizations out-source computer forensic problems?
15. Does the organization/department/agency you work for have policies for computer forensic readiness? If "YES", can you provide the name of your organization/department/agency? could you please briefly explain the policies.
16. In your country, are computer security issues and computer forensics issues dealt by different organization/department/agency? If "YES", how would you describe the relationship between computer security organization/department/agency and computer forensic organization/department/agency?

Section 5: Certification of Computer Forensics

17. How are computer forensic experts produced in your country? through what kind of tests? or procedures?
18. Do you allow computer forensic experts from other countries to work in a similar job in your country?
19. Does your country have any organization/department/agency for certifying computer forensic experts? If "YES", what are the names of the organizations/departments/agencies? What criteria do they follow?

Section 6: Training of Computer Forensics Experts

20. Is there any government organization/department/agency willing to support the education/training of computer forensic manpower? or to support the research of computer forensics? Can you briefly explain how the government organization/department/agency supports these agencies?
21. Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this program come from?
22. In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?
23. Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?

Section 7: Skills of Computer Forensic Experts

24. What is your opinion concerning the importance of hash functions in the field of computer forensics?
25. Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?
26. Based on your knowledge, what are the countermeasures within computer forensics to the collisions of hash functions?

Section 8: Bottlenecks within Computer Forensics

27. Based on your knowledge, have computer forensic investigations in your country ever encountered problems which are caused by time-stamps? or by different time zones? If "YES" how you deal this type of problems?
28. Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country?
    (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%
29. Based on your knowledge, how do computer forensic investigators deal with the encrypted data in your country?
30. Based on your knowledge, have performing computer forensic investigations in your country suffered any difficulty? Can you briefly list them?
31. "*Technical Issues*" and "*Human Issues*" are two separate things. It is easy to examine misuse of a computer, but how to prove the suspect is the one who actually caused this misuse is not an easy task. Based on your knowledge, how do computer forensic investigators deal with this problem in your country?

Section 9: Interaction in Computer Forensics

32. Based on your knowledge, have computer forensic organizations/departments/agencies in your country ever had interactions with international organizations/departments/agencies related to similar area? If "YES", how do they interact with other organizations/departments/agencies in other countries?
33. Based on your knowledge, in your country have computer forensic organizations/workers ever had interactions with other computer forensic organizations/workers? If "YES", how do they interact with each other?
34. Based on your knowledge, employees in the field of computer forensics normally interact or share their professional experiences with (1)colleague (2)supervisor

(3)others (please explain)

Section 10: Court Aspects of Computer Forensics

35. In your experience, do courts give a high or low weighting to digital evidence in your country?
36. Do you know of any difficulties caused by using digital evidence in court? If “SO”, what has been the major reason for this?
37. Based on your knowledge, is it the suspect’s obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If “YES”, Can you provide the name of the law?
38. Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If “SO”, does this affect the attitude of computer forensic investigators to perform investigations? If “YES”, can you briefly explain?

Section 11: Personal Preference of Computer Forensics Experts

39. As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?
40. As a computer forensic professional, do you use any type of encryption tools for the data in your work?

Appendix 2: Second Round Questionnaire for Delphi Survey in Australia (English Version)

1. In Australia, the development of computer forensics started around 8-10 years ago. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, How many years has computer forensics existed as a discipline in your country?, is Question 3 in Round One questionnaire.***)

   According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Years(time)	8 years	10 years	20 years	Many years	Unsure	Misunderstand
Number of Respondents	2	2	1	2	1	1

   1.1 Two experts think that computer forensics has been developed for 8 years.
   1.2 Two experts think that computer forensics has been developed for 10 years.
   1.3 One expert thinks that computer forensics has been developed for 20 years.
   1.4 Two experts think that computer forensics has been developed for many years.
   1.5 One expert is unsure about the answer.
   1.6 One expert misunderstands this question.

2. The situation of regulations may be different from state to state (from jurisdiction to jurisdiction), but there are regulations that define the time period to keep digital evidence after a trial. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?, is Question 7 in Round One questionnaire.***)

   According to the experts' opinions from Round One questionnaire, the conclusions are made in the table

Opinion	Yes, depending on the individual jurisdiction	No	Do not familiar with this issue
Number of Respondents	3	3	2

2.1 Three experts state that there has regulation about the time period to keep digital evidence after the trial. One of them says the default period is 7 years. The rest two experts say that the regulation mainly depends on the individual jurisdiction.

2.2 Three experts state there is no such regulation. However, two of them are not completely sure about this.

2.3 Two experts do not the answer of this question.

3. Do you agree with the characteristics of digital evidence within the following table? According to the table, the characteristics can be classified into 15 different categories. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what are the main characteristics of digital evidence? (e.g. Integrity), is Question 8 in Round One questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	Maintain chain of evidence	Relevant	Integrity
Number of Respondents	3	1	2
Opinions	Can be read by human	Can be interpreted by human	Can be authenticated
Number of Respondents	1	1	1
Opinions	Electronic form	Transient in nature	Volatile
Number of Respondents	2	1	1
Opinions	Must be reliable and accurate	Preservation	Interpretation
Number of Respondents	2	1	2
Opinions	Presentation	Correct and full analysis	
Number of Respondents	1	1	

4. Not every police station has an electronic crime section. Only federal-level and state-level police headquarters (e.g. AFP and SAPOL) have electronic crime sections. Thus, the status of computer forensic organization in law enforcement is higher than general police duties. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?, is Question 13 in Round One Delphi questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table

Opinions	Higher	Equal	No comment	Comparison is difficult
Number of Respondents	3	3	1	1

4.1 Three experts think that the status of computer forensic organization in law enforcement is higher than general police duties. For example, AFP.

4.2 Three experts think that the status of computer forensic organization in law enforcement is equal to general police duties. However, one of them is not very sure about this.

4.3 One expert has no comment for this question.

4.4 One expert thinks the comparison is difficult.

5. Although there is no clear method to train a computer forensic investigator, it takes around 2 years to train a computer forensic investigator. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?, is Question 23 in Round One questionnaire***.)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	6-18 months	2 years	5 years	Unsure	Depend
Number of Respondents	1	2	1	2	2

5.1 One expert thinks that it takes 6-18 months to train a computer forensic investigator.

5.2 Two experts think that 2 years is the reasonable time to properly train a computer forensic investigator.

5.3 One expert thinks it needs 5 years to train a computer forensic investigator.

5.4 Two experts are unsure about this question.

5.5 Two experts state that the answers change as the "levels" of computer forensic investigator vary.

6. In Australia, 0%-20% of computer forensic investigations encounter encrypted data. At most, 40% of computer forensic investigations encounter encrypted data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%, is Question 28 in Round One questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	0%-20%	21%-40%	Unsure or don't know this issue
Number of Respondents	4	1	3

6.1 Four experts think the reasonable percentage of encrypted data is 0%-20%.
6.2 One expert thinks the reasonable percentage of encrypted data is 21%-40%.
6.3 Three experts are not familiar with this issue.

7. In Australia, digital evidence is given a high weighting in court. Moreover, digital evidence is especially valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, In your experience, do courts give a high or low weighting to digital evidence in your country?, is Question 35 in Round One questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	High Weighting	Low Weighting	Treated as other types of evidence	Depends on the case
Number of Respondents	3	2	1	2

7.1 The number of experts choosing high weighting is more than the number of experts choosing low weighting.

7.2 One expert thinks that digital evidence is not treated any differently.

7.3 Two experts think that the weighting and acceptance of digital evidence are changed by cases. For example, the weighting of digital evidence is high in the computer crimes. On the contrary, the weighting of digital evidence is relatively low in the traditional cases.

8. The situation of computer-based legislation may be different from state to state (from jurisdiction to jurisdiction). Some legislation (such as the ***Cybercrime/Computer Crime Legislation 2001*** and ***Discovery in Common Law***) define the suspect's obligation for providing digital evidence within Australia. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, is it the suspect's obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If "YES", Can you provide the name of the law?, is Question 37 in Round One questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	Yes	No	Unsure
Number of Respondents	4	3	1

8.1 Four experts state that it is suspect's obligation to provide digital evidence. Two of them further point out the relevant legislation, and they are: ***Cybercrime/Computer Crime Legislation 2001***, and ***Discovery in Common Law***. However, one of them is not complete sure about his/her answer.

8.2 Three experts state that it is not suspect's obligation to provide digital evidence.

8.3 One expert is unsure about this question.

9. In Australia, some computer forensic experts do not use data wiping tools in their work for digital data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, As a computer forensic professional, do you use data wiper tools in your work for unnecessary data?, is Question 39 in Round One questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	Yes	No	No opinion or No answer
Number of Respondents	4	2	2

9.1 Four experts state that they do use data wiper tools for unnecessary data.

9.2 Two experts state that they do not use data wiper tools.

9.3 Two experts do not have answer for this question.

10. In Australia, some computer forensic experts do not use data encryption tools in their work for digital data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, As a computer forensic professional, do you use any type of encryption tools for the data in your work?, is Question 40 in Round One questionnaire.***)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	Yes	No	No opinion or No answer
Number of Respondents	4	3	1

10.1 Five experts state that they do use data encryption tools.

10.2 One expert states that he or she does not use data encryption tools.

10.3 Two experts do not have answer for this question.

Appendix 3: The Results of First Round Questionnaire for Delphi Survey in Australia (English Version)

Section 1: Conditions of Computer Forensics

1. From your point of view, what is your government's perspective on computer forensic issues? Do you think the emphasis they put on it is currently at an appropriate level?

   A. Does it have one? No I do not when cyber crime is now bigger than the drug trade we should equivalent or larger numbers of effort against this than drugs.
   B. I think there is growing realisation of the importance of the field.
   C. Computing forensic issues are complex, and this is recognized by government with several open and closed forums and working groups to debate the issues. The future of these is currently not certain, though.
   D. The Australian federal police is very involved with computer forensic issues. So are a number of large companies in Australia. I have no sense of a ratio between government financial investment and financial loss because of computer crime in any country, but data of this sort would be useful in getting a reasonable perspective on the issue.
   E. While there are some initiatives in place these are generally as a result of individual's initiative rather than government policy or encouragement. The government should be more proactive in setting guidelines for computer forensic practitioners.
   F. Computer forensics is considered an important forensic discipline and currently receives a reasonably strong emphasis.
   G. At a federal government level, a high priority is placed on computer forensics when matters involving terrorism or child pornography are concerned. This emphasis is in my view appropriate. At a state government level, there is less of a priority for computer forensics, principally due to other competing factors (e.g. street crime, crimes of violence etc.).
   H. Yes, right from the fields inception. A number of working parties have regularly met to ensure that the discipline is given all of the skills and resources that are needed for the discipline to be successful in Australia.

2. What is your opinion on the current developments within computer forensics? Are you satisfied with the current developments of computer forensics? Why?

   A. The move away from a strictly policing domain is a good one. A wider community of praxis should garner greater advances in theory and practice.
   B. I think that this is a complex issue complicated by political and budget issues. I am satisfied that things are happening but maybe not enough.
   C. Research is always ongoing, but it is a slow and reactive process. In some ways, it can never go fast enough.
   D. Formal education in computer forensics would be extremely useful in moving the area forward. A formalization as a recognized discipline with formal accreditation would be very good. However, these things tend to be driven by university (TAFE) programming and a perceived market for students rather than by government.
   E. There is insufficient focus on the growing problem of providing investigators with adequate tools to handle increasingly large datasets. Many challenges faced by investigators are due to rapidly changing and evolving technologies, which the tools cannot keep up with. As a result analysis of long-term needs of the community is weak.
   F. Computer forensics receives relatively little attention in most Australian academic institutions, consequently Australian research is not strong in this area.
   G. In terms of law enforcement, the developments within computer forensics are very good. There has been a strong focus on research and development, as well as national accreditation. Combined this has lead to a greater degree of autonomy for law enforcement, and therefore less reliance on third parties for solutions. In terms of the private sector, there is a distinct lack of progress with regard to computer forensics. This is due to the competing commercial interests and the strong reliance on third party commercial products.
   H. It is an ongoing process that more attention should be given.

3. How many years has computer forensics existed as a discipline in your country?

   A. 10+
   B. 10

C. Nominally, 1999 was the first academic publication, and although it was a practical area before then, it is at this time that it was probably codified as a discipline.
D. Formal university/TAFE programs still do not exist
E. Not sure.
F. It depends what you mean by "discipline". People have been extracting information from electronic devices for many years.
G. 20 years.
H. It has been practised seriously by practitioners since 1999/2000.

4. Is computer forensics a topical issue in your country?

A. Not really.
B. Yes.
C. Not really.
D. It is only for police and some IT academics.
E. Yes.
F. It depends on the audience you are considering.
G. Only when connected to Child pornography or terrorism.
H. Not as much as I would have thought. I think in general it is overlooked as a 'ture' forensic discipline (such as DNA, chemical analysis etc.). This will change in the future as NIFS get more involved.

Section 2: Procedures of Computer Forensics

5. From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?

A. There is not one unified statement/SOPs because of jurisdictional differences.
B. There is no national one but there are local ones.
C. There is no standard SOPs as far as I know – there are certain procedures that need to be followed and are well known, but some are lab-specific or dependent on a type of investigation.
D. This depends on the situation. This depends on whether it's a criminal or corporate situation and whether the scene is that of an individual machine or a network.

E. Not aware of any SOPs being used (I am not an investigator).
F. Each organization that carries out computer forensic investigations typically has its own SOPs. There are efforts underway under the auspices of NIFS to develop and agree standards for competencies and for tool validation and verification, however it is anticipated that (like any other field of endeavour) each organization will have its own particular style of practice.
G. SOPs are very much an individual matter. Each computer forensic team has its own particular SOPs. With recent moves to establish a national accreditation program, this should change. Common to most SOPs are the concepts of: evidence continuity, preservation of the original evidence, documentation, exhibit management, reporting, and case file management.
H. Each lab has their own seo of SOPs.

6. What is your opinion on the importance of SOPs of computer forensic investigations?

A. These are critical to demonstrate a wide range of compliance with principles and tenets of the discipline.
B. If these are not used then evidence is not robust for the court.
C. I believe that some form of procedure is necessary to ensure the integrity of the collection and analysis of data, but that is should not limit the investigative pathways of the analyst.
D. There should always be standard operating procedures.
E. Extremely important, if evidence is going to be used in court.
F. It is more important to have standards for competencies and for tool validation and verification than to try and force different organizations to use the same SOPs.
G. SOPs is critical to the forensic process. They provide a clear overview of the forensic process and as a consequence help define the underlying forensic methodology. All forensic teams should have SOPs.
H. Very important. To ensure that all forensic investigations are using accepted standard methods and procedures which may come under questions in a court of law.

7. Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?

   A. Yes depending on your individual jurisdiction within Australia there are differing requirements…all I will say I am glad I am not in QLD!
   B. I do think so..
   C. I do not know..
   D. I believe that the evidence must be returned immediately after a trial in which the defendant has been cleared.
   E. Don't know.
   F. It depends on the relevant legislation.
   G. The answer is very much dependent upon the matter under investigation. The typical default period is 7 years; however in some instances the court can order the destruction of data within a period that is less than 7 years.
   H. Not at this stage. We keep all digital evidence until the case is over and all avenges of appeal have been exhausted.

Section 3: Characteristics of Computer Forensics

8. Based on your knowledge, what are the main characteristics of digital evidence? (e.g. **Integrity**)

   A. No opinion.
   B. Must maintain chain of evidence.
   C. The integrity is important. Correct and full analysis and interpretation is also important.
   D. relevant, accurate, unaltered
   E. Unsure of intent of question. Digital evidence is characterized by its electronic nature. Chain of evidence is important to ensure it isn't modified after it is acquired. Due to the potentially massive volumes of data involved if can be difficult to analyse.
   F. This question is too vague to answer.
   G. Digital evidence: must be electronic form, must be capable of being read and interpreted in human form, must be capable of being authenticated, is transient in nature, is volatile, continuity must be able to be proved, and must be reliable.
   H. Preservation, Interpretation, and presentation.

9. What is your opinion on meta-data of digital evidence from computer forensic perspective?

   A. No opinion.
   B. Important to understand.
   C. It is important.
   D. If this means time stamps etc, they are extremely useful
   E. Meta data can be used to annotate digital evidence. It can also be contained within digital evidence (for example file meta-data) and can potentially contain information very useful to an investigation
   F. Metadata is a fundamental component of computer forensic evidence.
   G. Meta-data is critical to the computer forensic process. It is valuable for better understanding issues such as authenticity and ownership. Additionally, meta-data allows the forensic computer expert to undertake reconstructive analysis by facilitating a more reliable understanding of context as applied to electronic data. For example, MS Word meta-data allows the forensic examiner to better understand if a file was in fact created or modified as per the file system properties, as well as determine if a file is an original or a copy of an earlier instance of a file.
   H. It can be very useful. I use it regularly from MS WORD documents, and for the camera information contained in *.JPG picture files.

10. What is your opinion on the trustworthiness of meta-data of digital evidence?

   A. Yes.
   B. Yes.
   C. It can be incorrect, either accidentally (from clock drift or other environmental factors) or maliciously, but intentional manipulation of metadata is generally detectable and would be rare.
   D. There has to be clear evidence of their accuracy. It is easy to tamper with them.
   E. It depends on the nature of the meta-data. There is no reason why it should be any more or less trustworthy than other types of digital evidence. It can be easily manipulated (as can most digital evidence types). After proper processes, I think the trustworthiness of meta-data is OK.
   F. It depends. Dates and times are probably less reliable than some other forms of

metadata..

G. As with any electronic information, meta-data should not, in the first instance be deemed to be reliable. Usually some form of corroborating information is required to help determine the reliability of the meta-data.
H. In general, it is quite reliable. Unfortunately, windows vista now allows users to easily edit it, introducing a level of doubt.

11. How would you describe the relationship between computer security and computer forensics?

A. One is prevention of an incident; one is preservation of outcome of an incident.
B. A good understanding of security leads to sound forensics.
C. Computer security is proactive – preventative, whereas computer forensics is reactive – occurs after the fact.
D. Computer security attempts to keep people out of systems or communications; forensics deals with the situations where security fails..
E. Computer security is about protecting computing systems from unauthorized activities. Computer Forensics is about gathering and investigating evidence relating to unauthorized activities.
F. Computer forensics is typically misunderstood and confused with computer security.
G. Computer security predominantly focuses on preventative measures whilst computer forensics is very much reactive. In saying this, there is an overlap with regard to the design and implementation of a computer security incident response plan and the design of a computer forensic response plan. Consequently, whilst both focus on different aspects, they are connected by way of an incident response plan.
H. Completely different disciplines. Computer forensics would only be used after an attack.

12. When performing a computer forensic investigation, is it necessary to understand the background of the investigated person? (How many dogs they have? What cars they drive? Do they have any habit?) or just focus on analysing the digital data? Why?

A. Yes, corroborative sources of evidence or lines of enquiry.
B. Yes – forensic evidence can only be secondary.
C. It depends on the investigation – some evidence is either there or it is not, whereas some investigations may need information about the individual. I think having the information is helpful.
D. Yes. This is often the only way you can get passwords and relational material.
E. In many cases knowledge of the person under investigation might provide useful information to guide an investigator. Typically someone will only be investigated for a reason – therefore knowledge of the reason for the investigation and other background information about the suspect is vital.
F. It depends on what aspect is being investigated.
G. Knowing the background of the person(s) who uses or has access to the digital evidence is critical. Such information assists in profiling computer usage, and can aid in extrapolating ownership of digital evidence.
H. In general, No. 98% of the time, just details of the investigations and what is required is enough.

Section 4: Organization of Computer Forensics

13. In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?

A. No comment.
B. Higher.
C. It is different – the investigative areas have a higher rank than 'general duties', but there are also non-sworn analysts. The two areas are very different, and comparison is difficult.
D. Higher (AFP).
E. Unsure – I would guess equal.
F. It is no more or less important than other aspects of the organisation's work.
G. Computer forensics is regarded as an adjunct to any law enforcement activity. It is neither seen as higher or lower, but rather an integral component of the investigative process.
H. Higher. Computer forensic personnel reguire specific skills and can be called as expert witnesses.

14. In your country, do law enforcement organizations out-source computer forensic problems?

    A. No.
    B. Some in Federal government – not police.
    C. Not for criminal work.
    D. Yes. Often through corporations.
    E. When necessary.
    F. No.
    G. Law enforcement agencies, such as policing agencies, rarely outsource computer forensic analysis. Rather it is regulatory agencies such as the Australian Securities and Investment Commission and the Australian Competition and Consumer Commission that outsource most of their computer forensic collection and analysis functions.
    H. No, it is all done in-house.

15. Does the organization/department/agency you work for have policies for computer forensic readiness? If "YES", can you provide the name of your organization/department/agency? could you please briefly explain the policies.

    A. NA.
    B. No.
    C. I am unsure.
    D. Yes. At the auditing level. Deakin University has policies about auditing traffic flow and responding to anomalies.
    E. Not that I am aware of.
    F. Not that I am aware of.
    G. Yes. Organisation: <e.law> Australia Pty Ltd. The policy advises, in simple terms, that any computer security incident should be referred to the computer forensic team for immediate investigation. The SOPs of the computer forensic team deal with the incident response process.
    H. Not that I am aware of. I doubt that most agencies have even thought about it.

16. In your country, are computer security issues and computer forensics issues dealt by different organization/department/agency? If "YES", how would you describe the relationship between computer security organization/department/agency and computer forensic organization/department/agency?

A. YES. The strategic alignment of the security function and its role in the organisation.
B. Yes – collaborative - helpful.
C. There are several agencies that can deal with computer security issues, but have different focuses and jurisdictions. This depends on the state, the technology and a number of other factors.
D. Yes. Federal police and corporate forensic agencies collaborate.
E. Yes.
F. As outlined above, computer security is not the same as computer forensics. They are distinct, separate functions. In our organization they are treated separately.
G. This depends on the organisation/department/agency. In some law enforcement agencies the computer forensic function is managed by a different team to the computer crime and internal IT security teams. In other law enforcement agencies the computer crime team handles both computer forensics and computer crime investigations. In all law enforcement agencies, many of the internal IT security matters are handled by the IT department in the first instance. In some corporate organizations the IT department deals with all aspects of computer security issues and computer forensics.
H. The computer security agency is completely separated from the computer forensics sections.

Section 5: Certification of Computer Forensics

17. How are computer forensic experts produced in your country? through what kind of tests? or procedures?

A. Through the court.
B. Many means – no one standard. Experience is very important.
C. On-the-job and industry training. Incoming skill set depends on the lab.
D. They usually came through the police force and trained in IT.

E. University training, on-the-job training, some certification (mainly through the US).
F. In the context of forensics, the term “expert” is a status conferred on a witness by a court. Is that what you are referring to?.
G. Computer forensic experts are primarily produced by way of experience. Whilst there is some competency based testing at the law enforcement level, there is no formal and uniform testing program for the private sector.
H. Currently it is on-the-job. In the future, it will be formalized. So individuals will be required to conform to a set of competencies and be tested annually.

18. Do you allow computer forensic experts from other countries to work in a similar job in your country?

A. Yes.
B. Yes – (e.g. Jean Pierre Du Plessis).
C. Yes.
D. Yes.
E. Unsure – I would think so.
F. In our organization, computer forensic practitioners must be Australian citizens.
G. Yes. Subject of course to their experience and qualifications.
H. Have never been asked.

19. Does your country have any organization/department/agency for certifying computer forensic experts? If “YES”, what are the names of the organizations/departments/agencies? What criteria do they follow?

A. No.
B. No.
C. I do not know, but do not believe so.
D. No.
E. Unsure.
F. No. It currently appears unlikely that this will be the course of action which will be followed.
G. No.
H. NATA (see Q.17).

Section 6: Training of Computer Forensics Experts

20. Is there any government organization/department/agency willing to support the education/training of computer forensic manpower? or to support the research of computer forensics? Can you briefly explain how the government organization/department/agency supports these agencies?

    A. Yes they do. Allow people to train at Unis and also via grant schemes.
    B. NIFS and its Digital evidence Special Advisory group.
    C. Yes, for example NIFS.
    D. Not to my knowledge.
    E. The Australian Government supports the National Institute of Forensic Science. This group has a section devoted to computer forensics
    F. Our organization sponsors research by other government agencies and tertiary institutions through the same mechanisms that are used in other disciplines.
    G. In the private sector the role of training is very much up to individual organizations. Additionally alliances with academia assist in this regard.
    H. NIFS provides a number of 'small workshops' on topical issues. Vendor-based training is always available. The federal government (AFP) holds conferences from time to time.

21. Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this program come from?

    A. Yes there is. Often they are in-house experts.
    B. ON the job – plus commercial trainers – as required.
    C. I am unsure. I believe this is dependent on the individual lab.
    D. Only on an ad-hoc basis.
    E. Many LEAs provide on-the-job training for their staff.
    F. Ongoing training is important for all our computer forensic practitioners. This is typically sourced from external providers.
    G. We have an internal mentoring program that takes approximately 18 months to complete, subject of course to the capabilities of the individual..
    H. Am about to develop one.

22. In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?

    A. Yes, on-the-job training.
    B. Yes, on-the-job training is a popular way, but there is no standard method.
    C. I am unsure.
    D. Graduate degrees in forensics are available. At the undergraduate level there are some subjects.
    E. Some university courses are available. However, there is no standard qualification for computer forensic investigators in Australia.
    F. This question is too broad to answer.
    G. Yes. The majority of training is on-the-job training under the close supervision of a senior forensic practitioner.
    H. Vendor-based and on-the-job training.

23. Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?

    A. To what level of competency?.
    B. 5 years.
    C. I am unsure.
    D. Probably about 2 years.
    E. Unsure.
    F. It depends. We have different "levels" of practitioner.
    G. 6 months to a basic level. 18 months to an advance level.
    H. It is always on-going. It would take 2 years of training conbined with on-the-job training at least.

Section 7: Skills of Computer Forensic Experts

24. What is your opinion concerning the importance of hash functions in the field of computer forensics?

    A. They are important in most cases.
    B. If they don't understand this they can't do the work.
    C. They are vitally important.

D. They are very useful.
E. Hash functions provide an important mechanism for determining whether or not the data/evidence has changed since the time the hash was first applied.
F. Cryptographic hash techniques are fundamental to computer forensics.
G. Hash functions are used extensively to de-duplicate data, remove known files, and to identify flows of information (e.g. email chains). As such they have become an integral part of the forensic process.
H. It can be time-saving and important in 'proving' that files or forensic copies have not been modified.

25. Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?

A. These collisions were academic breaks per se but that said the use of a single hash is not advised. Taking a correct forensic approach verification and validation would dictate the use of 2 hashes or processes as minimum.
B. Makes evidence less robust – uncertainty brought in.
C. Hash collisions are rare, and do not necessarily invalidate findings. Also, combinations of hash functions are more robust.
D. Just use several hashes.
E. Hash functions for which collisions can be easily found should clearly not be used. Depending upon the particular situation the listed functions may still be ok. The problem is that non-technical people (such as court officials) may not understand the impact and easily be confused. If multiple hash functions, including one which is not known to suffer from collision weaknesses, are used then confusion can easily be avoided.
F. Research suggests that the MD5 collisions reported in the literature occur in contrived scenarios and as such do not pose a significant problem at this time. Nevertheless, technology continues to advance and new algorithms (e.g. SHA1) provide larger key spaces that reduce the chances of collisions and it is possible that the world wide community of computer forensic practitioners will gradually transition to these new algorithms.
G. Whilst collisions open the possibility of errors in the forensic process, the probability of such collisions occurring is still relatively low. Despite this

however, there is emerging a need to show that the forensic process has not been undermined by a HASH collision.

H. Neglegible, as those collissions were on small files. We use the combinations of MD5/SHA1 to avoid this argument.

26. Based on your knowledge, what are the countermeasures within computer forensics to the collisions of hash functions?

A. See 25.
B. Don't know - none.
C. Use of multiple hash functions in conjunction.
D. Use several hashes. No-one has yet shown collisions on the same documents across two or more hash functions.
E. Apply multiple hash functions at the time of acquisition.
F. This question is unclear..
G. The two most common methods used: For a small number of files, direct binary comparison. For a large number of files, either use a "collision free" HASH (e.g. SHA1) or use a combined HASH value made up of both MD5 and SHA.
H. See Q25.

Section 8: Bottlenecks within Computer Forensics

27. Based on your knowledge, have computer forensic investigations in your country ever encountered problems which are caused by time-stamps? or by different time zones? If "YES" how you deal this type of problems?

A. YES. Other data sources…or use of another method to prove guilt or innocence.
B. Yes.
C. Yes- there have been issues in forensic applications that have not accounted for local time zones correctly. Eventually, a patch was released.
D. I do not know.
E. Not aware of any such problems, but would suspect to be highly likely
F. Yes, these are typically dealt with through manual procedures.
G. YES. Time zones: Two time related issues emerge in Australia. The first is time zones, and the other is Daylight Savings (e.g. Between NSW and QLD). In such cases the forensic analysis is conducted on a computer configured to the time

zone settings of the original PC. In addition to this, I often work in UTC format, converting to local time as required. Time-Stamps: Time stamps can and do present a wide range of forensic issues. The first issue to consider is the reliability of the time stamp. In particular, has it been affected by human manipulation. The second issue to consider is has a third party product (e.g. virus scanner) impacted on the time stamps.

H. Nothing that has affected me. .

28. Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country?
(1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%

A. 0%-20%.
B. Don't know
C. 0%-20%.
D. My guess is (2).
E. Not sure.
F. No answer.
G. 0%-20%
H. (0%-20%) do not tell anyone.

29. Based on your knowledge, how do computer forensic investigators deal with the encrypted data in your country?

A. They don't largely apart from throwing it a large cracking engines/clusters.
B. Decryption by different means.
C. Depends on whether the data within the encrypted file is of use. There are also applications such as FTK that break passwords.
D. Password cracking or guessing are the two most common approaches.
E. Ask for keys. Brute force (dictionary search for key).
F. No answer.
G. Typically through one of three mechanisms: Software based decryption software, Hardware based decryption accelerators, or compelling an entity to divulge a password by means of a legal instrument (e.g. court order).
H. We throw all the tools and computing power we can at it.

30. Based on your knowledge, have performing computer forensic investigations in your country suffered any difficulty? Can you briefly list them?

    A. Yes. Human.
    B. Yes. The number of computer forensic investigator is not enough.
    C. Resources, include manpower and equipment, are not enough.
    D. Probably lack of resources – people and equipment.
    E. Not sure.
    F. No answer.
    G. Difficulties include: unusual or proprietary data formats, extracting data from proprietary legacy systems, corrupted data, timely processing of large volumes of data (particularly with respect of backup tapes), deliberate destruction or manipulation of data by a third party prior to seizure, encrypted data, faulty forensic software, unrealistic deadlines set by the courts, and unrealistic expectations by lawyers.
    H. Password protected hard disk drives.

31. "Technical Issues" and "Human Issues" are two separate things. It is easy to examine misuse of a computer, but how to prove the suspect is the one who actually caused this misuse is not an easy task. Based on your knowledge, how do computer forensic investigators deal with this problem in your country?

    A. No opinion.
    B. Use other types of evidence.
    C. This is sometimes called the last mile. If passwords are accessed, such as for online banking, this will tie computer use back to an individual. Similarly, if emails are sent from an account belonging to the user, this is also of use.
    D. By gathering as much related evidence as possible to link the person to the crime.
    E. In practice it is likely that investigators will rely on more than just computer based evidence in an investigation. Computer evidence is likely to support other evidence, rather than be the sole source of evidence for a prosecution.
    F. In our organization, computer forensic examiners work hand-in-hand with investigators (we do not combine the functions). As such it is up to the investigators to seek corroboration through other means.

G. In order to establish a nexus between a person's logical identity (e.g. user login) and their physical identity is problematic. To address this issue, we often try to identify a behaviour that is unique to a person (e.g. sending a personal email to friends) and hypothesizing that any logical activity occurring around this event was done by the individual. Other techniques include profiling known user behaviours and linking them to the logical events. Additionally, we link in other known events (e.g. access logs on office security, eye witness accounts, surveillance camera footage etc.) with the suspect logical activity.
H. Look for usage of the computer by the individual.

Section 9: Interaction in Computer Forensics

32. Based on your knowledge, have computer forensic organizations/departments/agencies in your country ever had interactions with international organizations/departments/agencies related to similar area? If "YES", how do they interact with other organizations/departments/agencies in other countries?

A. YES. It varies.
B. Yes – don't know but through treaties and Interpol.
C. Yes.
D. Yes. They collaborate with comparable overseas organizations.
E. Not sure.
F. Yes, our organization maintains relationships with many international law enforcement agencies.
G. Yes. Interaction occurs either by way of personal relationships and or formal committees.
H. Not in our area.

33. Based on your knowledge, in your country have computer forensic organizations/workers ever had interactions with other computer forensic organizations/workers? If "YES", how do they interact with each other?

A. Yes. Often.
B. Yes – through NIFS and Fed Govt.
C. Unsure.

D. They consult.
E. Yes. Through groups such as the "Digital evidence Innovation Network" a collection of research groups and LEAs. Through collaborative and contract research projects.
F. Yes. Our organization sponsors research by Australian tertiary institutions.
G. Yes. Interaction is primarily via personal relationships.
H. Yes, we have a partnership with UniSA. I believe that WAPOL have a partnership with the Edith Cowan University.

34. Based on your knowledge, employees in the field of computer forensics normally interact or share their professional experiences with (1)colleague (2)supervisor (3)others (please explain)

A. 1, 2, and 3.
B. 1, and 2.
C. 1, and 2. There are several forums and specialized groups, and it may be that experiences are shared within these areas.
D. To the extent that the work is confidential, experience is not shared. However, experience with tools and methodologies are shared.
E. Within Queensland LEAs have formed the Queensland Digital Evidence Group which meets regularly, occasionally inviting outside experts to contribute.
F. This question is unclear.
G. 1, and 2. In the private sector, interaction by way of personal relationships results in the exchange of knowledge and solutions. There are no formal industry bodies for which formalised interaction takes place.
H. It is kept pretty close to the chest (1) Yes, (2) Yes, and (3) Maybe with other law enforcement agencies only.

Section 10: Court Aspects of Computer Forensics

35. In your experience, do courts give a high or low weighting to digital evidence in your country?

A. High.
B. High.
C. Depends on the case. It is given some weighting..

D. Low.
E. Relatively low – digital evidence is usually considered to be “circumstantial”.
F. It depends. All forensic evidence is circumstantial.
G. A high weight.
H. I do not think it is treated any differently.

36. Do you know of any difficulties caused by using digital evidence in court? If “SO”, what has been the major reason for this?

A. Yes.
B. Yes, understanding of digital evidence.
C. Yes, not enough knowledge.
D. Lawyers and judges do not understand information technologies.
E. Not sure.
F. It is sometimes difficult to explain complex technical evidence in court.
G. Yes. The primary difficulty appears to be an understanding, by the courts and lawyers, of the forensic and technical issues associated with the extraction and analysis of digital evidence.
H. Non that I have experienced. Audio visual/computer facilities would be advantageous.

37. Based on your knowledge, is it the suspect’s obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If “YES”, Can you provide the name of the law?

A. No.
B. Yes –Cybercrime/Computer Crime Legislation 2001.
C. I believe yes, but am not sure.
D. No.
E. Not sure.
F. Not that I am aware of but this is not my area of expertise.
G. In terms of civil discovery, both parties are obliged to exchange evidence pertaining to the matter in dispute. This is governed by a series of Federal Court and state court practice notes.
H. Yes, our detectives hold ‘general search warrants’.

38. Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If “SO”, does this affect the attitude of computer forensic investigators to perform investigations? If “YES”, can you briefly explain?

A. Yes. Computer forensic investigators have to do their works without any influence.
B. Yes. Insufficient laws do not affect the attitudes of computer forensic investigators.
C. Yes. I do not think the attitudes of computer forensic investigators are affected by incompletion of laws.
D. Lawyers and judges do not understand information technologies. In addition, the law does not apply to some digital situations.
E. Not sure.
F. This question is not clear.
G. Yes. With recent advances in concept searching and correlation analysis, the reliability of the output is not guaranteed under the existing evidence provisions. Despite this however, this is not an inhibitor to using such techniques, but rather it places a greater onus on the forensic examiner to explain and validate the underlying process.
H. The laws will never keep up. The development of law does not affect my job.

Section 11: Personal Preference of Computer Forensics Experts

39. As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?

A. Yes.
B. No opinion.
C. Yes, when necessary.
D. Yes.
E. No.
F. No answer.
G. Yes.
H. No.

40. As a computer forensic professional, do you use any type of encryption tools for the data in your work?

A. No.
B. No.
C. Not personally.
D. Yes.
E. Yes.
F. No answer.
G. Yes.
H. Yes, for sensitive material, encryptions are employeed on CD/DVD’s.

Appendix 4: The Results of Second Round Questionnaire for Delphi Survey in Australia (English Version)

1. In Australia, the development of computer forensics started around 8-10 years ago. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, How many years has computer forensics existed as a discipline in your country?, is Question 3 in Round One questionnaire*.)**

    A. Unsure.
    B. Agree.
    C. I would agree with this statement.
    D. YES.
    E. Yes.
    F. Yes, that sounds reasonable.
    G. Yes.
    H. From my knowledge, I still say that it has been practised seriously in Australia for about 9 years now.

2. The situation of regulations may be different from state to state (from jurisdiction to jurisdiction), but there are regulations that define the time period to keep digital evidence after a trial. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?, is Question 7 in Round One questionnaire*.)**

    A. Agree.
    B. I agree with this statement since this is definitely true in Australia.
    C. Not familiar with this issue.
    D. YES.
    E. Yes.
    F. Yes, but don't know specifics.
    G. Yes.

H. The government archival standard for documents is 7 years so I guess that the same would apply to evidence. It is my practise to keep the evidence for as long as is practically possible. ie. Forever.

3. Do you agree with the characteristics of digital evidence within the following table? According to the table, the characteristics can be classified into 15 different categories. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what are the main characteristics of digital evidence? (e.g. Integrity), is Question 8 in Round One questionnaire*.)**

   A. Agree.
   B. Yes.
   C. Yes.
   D. YES.
   E. Yes.
   F. Don't understand your question
   G. Yes.
   H. YES, I agree. They are all valid.

4. Not every police station has an electronic crime section. Only federal-level and state-level police headquarters (e.g. AFP and SAPOL) have electronic crime sections. Thus, the status of computer forensic organization in law enforcement is higher than general police duties. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, In your country, is the status of computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?, is Question 13 in Round One Delphi questionnaire.***)

   A. Agree.
   B. Yes.
   C. I agree with the information on the table.
   D. YES.
   E. Yes.

F. I don't understand what you mean by "status". Both policing and forensic functions are important
G. Yes.
H. As the discipline requires specific expert knowledge it has to be higher

5. Although there is no clear method to train a computer forensic investigator, it takes around 2 years to train a computer forensic investigator. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?, is Question 23 in Round One questionnaire.***)

A. Agree.
B. Yes. I think the continuous training program is important as well.
C. Yes. In addition, I think training is an ongoing process and needs to be continually revised over time
D. No, 6-18 months depending on skills.
E. Yes.
F. I believe it can take 2 years for someone to become competent with a reasonable IT background to become in the basics of CF and understand how to work within their organisation. That said, the AFP employs CF practitioners at several different levels which reflect their responsibilities.
G. Yes.
H. You can give a computer forensics investigator basic training in 6 months, enough to do the work, but they really don't know what they are doing and what is achievable until 2 years doing the work.

6. In Australia, 0%-20% of computer forensic investigations encounter encrypted data. At most, 40% of computer forensic investigations encounter encrypted data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%, is Question 28 in Round One questionnaire.***)

A. Agree.
B. Unsure
C. Unsure – this is not my field of study.
D. YES.
E. Yes.
F. YES.
G. Yes.
H. I rarely see encrypted data. 0-20% definitely over here.

7. In Australia, digital evidence is given a high weighting in court. Moreover, digital evidence is especially valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, In your experience, do courts give a high or low weighting to digital evidence in your country?, is Question 35 in Round One questionnaire*.)**

A. Agree.
B. Yes.
C. Unsure.
D. YES.
E. Yes.
F. It depends. I don't believe there is any hard and fast rule here
G. Yes.
H. High Weighting.

8. The situation of computer-based legislation may be different from state to state (from jurisdiction to jurisdiction). Some legislation (such as the ***Cybercrime/Computer Crime Legislation 2001*** and ***Discovery in Common Law***) define the suspect's obligation for providing digital evidence within Australia. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, is it the suspect's obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If "YES", Can you provide the name of the law?, is Question 37 in Round One questionnaire*.)**

A. Agree.
B. Yes.
C. Unsure.
D. YES.
E. Yes.
F. I don't understand this question
G. Yes.
H. Yes. However, from my perspective, I don't think there is any obligation specific to digital evidence. Evidence is evidence – it just happens to be digital.

9. In Australia, some computer forensic experts do not use data wiping tools in their work for digital data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, As a computer forensic professional, do you use data wiper tools in your work for unnecessary data?, is Question 39 in Round One questionnaire*.)**

A. Agree.
B. Yes.
C. Unsure.
D. YES.
E. Yes.
F. It depends. Wiping is appropriate in some situations (e.g. restoring a copy of a disk to blank media) but may not be necessary in others (e.g. making a copy of a source disk using dd or EnCase format)
G. Yes.
H. Yes, I agree with the statement. There are times where data wiping tools are needed to conduct our day-to-day work in a 'clean-room' environment. But, in general we are in the business of preserving data.

10. In Australia, some computer forensic experts do not use data encryption tools in their work for digital data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, As a computer forensic professional, do you use any type of encryption tools for the data in your work?, is Question 40 in Round One questionnaire*.)**

A. Agree.

B. Yes.

C. Unsure.

D. YES.

E. Yes.

F. Cannot comment

G. Yes.

H. Yes. In my case, I use encryption to protect sensitive data.

Appendix 5: First Round Questionnaire for Delphi Survey in Taiwan (Chinese Version)

Section 1: 數位鑑識(Computer Forensics)的情況

1. 依您所見，官方(政府)單位對於數位鑑識的觀點為? 您認為官方(政府)單位是否適當地重視此議題?
2. 您對現今數位鑑識發展的看法? 您對於現況感到滿意嗎? 請簡單說明
3. 數位鑑識在貴國成立的年數(時間)有多久?
4. 數位鑑識在貴國算是熱門的議題嗎?

Section 2: 數位鑑識的步驟

5. 依您所見，在貴國執行數位鑑識時可以依循的標準程序(Standard Operation Procedure)為何?
6. 您對於數位鑑識標準程序(SOPs)之重要性的看法?
7. 據您所知，是否有條文規範數位證據(digital evidence)在開庭過後需要保存多久時間? 如果有，期限為?

Section 3: 數位鑑識的特徵

8. 據您所知，數位證據的主要特性是什麼? (例如: 一致性(Integrity))
9. 從數位鑑識的觀點來說，您怎麼看待數位證據中所呈現的中介資料(meta-data)?
10. 您認為數位證據中所呈現的中介資料的可信度(trustworthiness)為何?
11. 您認為資訊安全(computer security)跟數位鑑識(computer forensics)兩者之間的關係為何?
12. 當執行數位鑑識的調查時，您認為需不需要了解被調查者的背景? (例如：有

幾隻狗? 開什麼車? 有什麼興趣?) 還是專注於分析數位資料? 請簡述原因

Section 4: 數位鑑識的組織

13. 貴國執法體系中數位鑑識單位的層級是高於一般警局? 還是等於? 還是低於?
14. 貴國的執法單位有將數位鑑識進行委外處理嗎?
15. 您的工作單位對於數位鑑識是否有所準備? 如果有，請您提供貴單位的名稱。 同時，請您簡單說明這些政策。
16. 在貴國， "資訊安全的議題" 和 "數位鑑識的議題" 是否由不同的單位來處理? 如果是，請您說明貴國 "資訊安全的單位" 跟 "數位鑑識的單位" 兩者之間的關係為何?

Section 5: 數位鑑識的的認證

17. 貴國的數位鑑識專家是如何形成的? 是透過何種測驗? 或是透過何種步驟??
18. 貴國是否接受他國的數位鑑識專家前來從事相關工作?
19. 貴國是否有 "某個單位" 對於數位鑑識專家進行認證? 如果有，此單位的名稱為? 所依循的標準為何?

Section 6: 數位鑑識專家的訓練

20. 政府相關部門是否願意舉辦活動支持數位鑑識從業人員的教育 or 訓練? 是否支持數位鑑識的研究? 請您簡單說明政府相關部門是如何支持這類活動。
21. 就您所知，貴國有提供數位鑑識調查員的在職訓練嗎? 通常多久舉辦一次? 師資來源為?
22. 貴國有沒有訓練數位鑑識專家的方法? 如果有，請您簡述之

23. 根據貴國數位鑑識發展的現況，您認為訓練依各數位鑑識調查員所需的時間是多久?

Section 7: 數位鑑識專家的技巧

24. 在數位鑑識的領域中，您對於雜湊函數(hash function)的重要性有何看法?
25. 某些雜湊函數的碰撞已經被證實(例如 MD4, MD5, and SHA0)，您認為雜湊函數的碰撞對於數位鑑識有什麼影響?
26. 就您所知，以數位鑑識的觀點來看，對於雜湊函數的碰撞有什麼對策?

Section 8: 數位鑑識的瓶頸

27. 就您所知，貴國的數位鑑識調查行動是否有遭遇到由時戳(time-stamp) 所以起的困擾? or 遭遇到由不同時區(different time zones)所以起的困擾? 如果有，您習慣如何處理這類問題?
28. 就您所知，貴國數位鑑識調查行動所遭遇到的加密資料其百分比為何?
    (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%
29. 就您所知，貴國的數位鑑識調查員如何處理加密的資料?
30. 就您所知，貴國的數位鑑識調查行動是否有遭遇任何困難? 請您簡單條列
31. “技術” 和 “人” 是兩各不同的層面。單純檢驗電腦上的濫用是簡單的，然而如何證明嫌疑犯就是濫用電腦的人則相對困難。就您所知，貴國的數位鑑識調查員是如何處理這類的問題?

Section 9: 數位鑑識的交流

32. 就您所知，貴國的數位鑑識組織是否有跟國際的相關組織做交流? 如果有，

請問交流的方式為何?

33. 就您所知，貴國的數位鑑識組織/學者是否有與貴國的相關數位鑑識組織/學者做交流? 如果有，請問交流的方式為何?

34. 就您所知，數位鑑識這方面的工作人才通常將其專業經驗與何人交流?

(1)同事 (2)長官 (3)其他(請說明)

Section 10:法庭對數位鑑識的觀點

35. 以您的經驗，法庭對於數位證據的重視度(採性度)是高? 是低?

36. 就您所知，在法庭上使用數位證據是否有遭遇任何困難? 如果有，造成這情形的主要原因為?

37. 就您所知，在貴國嫌疑犯是否有義務提供數位證據? 貴國是否有哪一部法律有規範這樣的義務? 如果有，那部法律的名稱是?

38. 就您所知，貴國是否有現行法律跟不上數位鑑識的發展之現象? 如果有，這是否影響數位鑑識調查員的辦案態度? 如果有，請簡述

Section 11: 數位鑑識專家的工作習性

39. 身為數位鑑識專家，在工作上對於不必要的資料，您是否會使用資料清除工具?

40. 身為數位鑑識專家，對於工作上的資料，您是否會使用加密工具?

Appendix 6: Second Round Questionnaire for Delphi Survey in Taiwan (Chinese Version)

1. 在台灣，數位鑑識這個議題的發展約在 4~5 年前。至於相關數位鑑識實驗室則是於 2006 年底建立。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 3 題：數位鑑識在貴國成立的年數(時間)有多久?***)

   在第一回合中專家答案如表所列，並且分析整理如下:

年數(時間)	0.5 年	2 年	4-5 年	7-8 年	不清楚
作答人數	1	1	4	2	2

   1.1 一位專家認為，既然調查局數位鑑識實驗室建立於 2006.12.26，所以算起來僅有半年左右。

   1.2 一位專家認為，近兩年來國內才對數位鑑識這個議題有所共識。

   1.3 四位專家認為，數位鑑識這個議題發展迄今大約 4-5 年。

   1.4 兩位專家認為，數位鑑識這個議題約在 7-8 年前開始發展。

   1.5 兩位專家並不清楚這個議題。

2. 在台灣，基於認知的不同或是單位的不同，目前有多套標準可以參考(由 2.1 可以看出)，但是一個明確的數位鑑識 SOPs 並不存在。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 5 題：依您所見，***

在貴國執行數位鑑識時可以依循的標準程序(Standard Operation Procedure) 為何?)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	認為有 SOPs	認為沒有 SOPs	不清楚
作答人數	5	3	2

2.1 五位專家認為，在台灣有可以依循的 SOPs。條列如下:

A: Preparation, Documentation, Collection, Authentication, Analysis, Preservation, Production, and Reporting.

B: 沿用警察大學林宜隆所提出的程序以及效法美國的程序。

C: 普遍依循警政單位所遵守的蒐證原則。

D: 警察偵查犯罪規範 第六章第 14 節。

E: 蒐集、採證、分析、報告、法庭呈現。

2.2 三位專家認為，在台灣目前並沒有統一的 SOPs 可以依循。

2.3 兩位專家並不清楚這個議題。

3. 數位證據的主要特性可以被歸類為 12 項(由以下圖表可知)。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 8 題：據您所知，數位證據的主要特性是什麼? 例如: 一致性(Integrity)***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	一致性(同一性)	完整性	易破壞	可無限複製	原始資料不可讀	使用者不易確定
作答人數	5	3	6	5	3	3
意見	不易取得	具備證據能力	多樣性	不易銷毀	不可否定性	具有中介資料
作答人數	1	2	1	1	1	1

4. 數位證據中所呈現的中介資料(例如：時戳)，在數位調查中扮演著相當重要的角色。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 9 題：從數位鑑識的觀點來說，您怎麼看待數位證據中所呈現的中介資料(meta-data)?***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	重要	誤解題意	不了解問題	不清楚	無意見
作答人數	4	3	1	1	1

4.1 四位專家認為，中介資料是重要的，可以提供額外的資訊，也是數位證據所獨有的特點。例如：時戳(time-stamp)即為典型的數位證據中介資料。

4.2 三位專家誤解了題意。

4.3 一位專家不了解問題。

4.4 一位專家並不清楚這個議題。

4.5 一位專家對此題無意見(未作答此題)。

5. 只要符合程序並且使用合格的工具，數位證據中所呈現的中介資料的可信度將不是問題。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 10 題：您認為數位證據中所呈現的中介資料的可信度 (trustworthiness)為何?***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	可信度高	可信度視情形而定	不了解問題	不清楚	無意見
作答人數	3	4	1	1	1

5.1 三位專家認為，中介資料的可性度相當高。

5.2 四位專家認為，中介資料的可性度視情形而定。例如：鑑識工具的公信力，資料是否完整皆會影響其可性度。

5.3 一位專家不了解問題。

5.4 一位專家並不清楚這個議題。

5.5 一位專家對此題無意見(未作答此題)。

6. 一般來說，在台灣，實務單位(例如：法務部調查局)對於數位鑑識是有所準備，然而非實務單位(例如：各大學)對於數位鑑識並相同的準備也沒有相同的需求。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 15 題：您的工作單位對於數位鑑識是否有所準備? 如果有，請您提供貴單位的名稱。同時，請您簡單說明這些政策。***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	有準備	沒有準備
作答人數	4	6

6.1 四位專家任職於實務單位，而這些單位對於數位鑑識皆有所準備。

6.2 六位專家任職於非實務單位，而這些單位對於數位鑑識並沒有準備。其中有兩位任職於學校的專家，認為學校對於數位鑑識並沒有迫切的需求。

7. 在台灣，確實有提供數位鑑識調查員的在職訓練，主要是不定期。師資來源雖然都是數位鑑識領域的專家，但是並不是單一來源。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 21 題：就您所知，貴國有提供數位鑑識調查員的在職訓練嗎? 通常多久舉辦一次? 師資來源為?***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	有	不清楚
作答人數	6	4

7.1 六位專家表示在台灣是有提供數位鑑識調查員的在職訓練。其中四位專家表示這類訓練是不定期的。其中一位專家表示這類訓練在其服務單位是一年一次。至於師資部份，其中一位專家表示師資來自於調查局或刑事局資深人員。另一位專家表示師資來自於國內外從事數位鑑識相當專業的廠商或是專業人員來授課。

7.2 四位專家並不清楚這個議題。

8. 訓練一個調查員成為數位鑑識調查員所需的時間至少為一年。在此之後，數位鑑識調查員必須持續學習。您對於這樣的說法是否贊成? 請簡述原因。您

尚有其他意見嗎? (***原第一回合第 23 題：根據貴國數位鑑識發展的現況，您認為訓練一個數位鑑識調查員所需的時間是多久?***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	高標準	持續不間斷	以年計	以月計	不清楚
作答人數	1	2	4	1	2

8.1 一位專家認為，應該是高規格、高標準。但是並沒有說明確切的時間。

8.2 兩位專家認為科技不停地進步，因此訓練一個數位鑑識調查員是持續不間斷地。

8.3 四位專家認為，訓練一個數位鑑識調查員所需的時間至少是一年。

8.4 一位專家認為，訓練一個數位鑑識調查員所需的時間為 2-3 個月。

8.5 兩位專家並不清楚這個議題。

9. 雜湊函數的碰撞對於數位鑑識是有影響的。這些影響可能包括：數位證據之證據力受到質疑、增加數位鑑識的難度。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎?(***原第一回合第 25 題：某些雜湊函數的碰撞已經被證實(例如 MD4, MD5, and SHA0)，您認為雜湊函數的碰撞對於數位鑑識有什麼影響?***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	有影響	沒有影響	不清楚
作答人數	6	1	3

9.1 六位專家認為，雜湊函數的碰撞對數位鑑識是有影響的。可能的影響為：數位證據之證據力受到質疑、增加數位鑑識的難度。

9.2 一位專家認為，雜湊函數的碰撞對數位鑑識是沒有影響的。

9.3 三位專家並不清楚這個議題。

10. 在台灣，數位鑑識調查行動所遭遇到的加密資料其百分比應該是相對偏低(0%-20%)，至多不會超過 40%。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎?(***原第一回合第 28 題：就您所知，貴國數位鑑識調查行動所遭遇到的加密資料其百分比為何? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	0%-20%	21%-40%	41%-60%	不清楚	無意見
作答人數	4	1	1	3	1

10.1 四位專家(其中兩位有實務經驗)認為，加密資料的百分比應該為 0%-20%。

10.2 一位專家認為，加密資料的百分比應該為 21%-40%。而此經驗為實際辦案所獲得。

10.3 一位專家認為，加密資料的百分比應該為 41%-60%。

10.4 三位專家並不清楚這個議題。

10.5 一位專家對此題無意見(未作答此題)。

11. 在台灣，法庭雖然無法忽略數位證據的重要性，但是法庭普遍來說對於數位證據的採性度偏低。特例是，如果是電腦犯罪，則有關犯罪的數位證據的重視度以及採性度應該是相當高。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 35 題：以您的經驗，法庭對於數位證據的重視度(採性度)是高? 是低?***)

在第一回合中專家答案如表所列，並且分析整理如下:

意見	重視度高	重視度低	視情況而定
作答人數	4	4	2

意見	採性度高	採性度低	視情況而定
作答人數	2	6	2

11.1 在重視度方面，選擇"重視度高"的專家人數和選擇"重視度低"的專家人數一樣。

11.2 在採性度方面，選擇" 採性度低"的專家人數明顯多於選擇"採性度高"的專家人數。

11.3 兩位專家表示數位證據的重視度以及採性度隨案件性質不同而有所不同。如果是電腦犯罪，則有關犯罪的數位證據的重視度以及採性度應該是相當高，相對的，如果是一般刑事犯罪，則數位證據的重視度以及採性度則應該較低。

Appendix 7: Second Round Questionnaire for Delphi Survey in Taiwan (English Translation)

1. In Taiwan, computer forensics was developed around 4~5 years ago, and the Cyber Forensics Laboratory was established at the end of 2006. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, How many years has computer forensics existed as a discipline in your country?, is Question 3 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Years(time)	0.5 year	2 years	4-5 years	7-8 years	Do not familiar with this issue
Number of Respondents	1	1	4	2	2

1.1 One expert thinks the answer of this question is around 0.5 year since the cyber forensics laboratory was built on 26/12/2006.

1.2 One expert thinks that the consensus of computer forensics is made around 2 years ago. This means the answer of this question is 2 years.

1.3 Four experts think that computer forensics has been developed for 4-5 years.

1.4 Two experts think that computer forensics has been developed for 7-8 years.

1.5 Two experts do not familiar with this issue.

2. Due to different organizations and/or different understandings, there is more than one guidelines for computer forensics (confirmed by 2.1). Unfortunately, there is no specific SOPs for computer forensic purpose at this moment. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?, is* Question 5 in Round One questionnaire.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table

Opinion	SOPs	No SOPs	Do not familiar with this issue
Number of Respondents	5	3	2

2.1 Five experts think that the SOPs are indeed existed, and they provide five different SOPs. These SOPs are listed as follow.

A: Preparation, Documentation, Collection, Authentication, Analysis, Preservation, Production, and Reporting.

B: The SOPs mainly consists of the concepts proposed by I-Long Lin who works in central police university, and some ideas form America.

C: From my understanding, evidence collecting principles for law enforcement are normally used as SOPs for computer forensics.

D: Section 14 of Chapter 6, Investigating Principles for Police Force

E: Collecting, analysing, reporting, and presenting

2.2 Three experts think there is no unified SOPs in Taiwan.

2.3 Two experts do not know the answer of this question

3. According to the table, the characteristics can be classified into 12 different categories. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what are the main characteristics of digital evidence? (e.g. Integrity), is Question 8 in Round One questionnaire*.**)

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	Consistency	Integrity	Easy to damage
Number of Respondents	5	3	6
Opinions	Hard to retrieve	Admissibility	Diversity
Number of Respondents	1	2	1
Opinions	Able to duplicate	Original data is not understandable	Hard to identify users
Number of Respondents	5	3	3
Opinions	Hard to eliminate	Non-Repudiation	Contain meta-data
Number of Respondents	1	1	1

4. The meta-data (e.g. time stamp) of digital evidence plays an important role in a computer forensic investigation. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, What is your opinion on meta-data of digital evidence from computer forensic perspective?, is Question 9 in Round One questionnaire.*****)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	Important	Misunderstand the question	Do not understand the question	Do not familiar with this issue	No Opinion
Number of Respondents	4	3	1	1	1

4.1 Four experts think that meta-data is important since meta-data can offer additional information. This is also the uniqueness of digital evidence. For example, time-stamp is one typical type of meta-data.

4.2 Three experts misunderstand the meaning of this question.

4.3 One expert does not understand the meaning of this question.

4.4 One expert does not familiar with this issue.

4.5 One expert does not answer this question.

5. As long as the procedures and computer forensic tools are correct, the reliability of meta-data of digital evidence is not a problem. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, What is your opinion on the trustworthiness of meta-data of digital evidence?, is Question 10 in Round One questionnaire***.**)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	High Trustworthiness	Depend on the situation	Do not understand the question	Do not familiar with this issue	No Opinion
Number of Respondents	3	4	1	1	1

5.1 Three experts think the trustworthiness of meta-data is relative high.

5.2 Four experts think that the trustworthiness of meta-data depends on the different situations. For example, the credibility of computer forensic tools, and the completeness of the original data.

5.3 One expert does not understand the meaning of this question.

5.4 One expert does not familiar with this issue.

5.5 One expert does not answer this question.

6. Generally speaking, in Taiwan, practical organizations (e.g. MJIB) have facilities, processes, and ability for computer forensic issues, but non- practical organizations (e.g. university) do not have equivalent preparations and needs. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Does the organization/department/agency you work for have policies for computer forensic readiness? If "YES", can you provide the name of your organization/department/agency? could you please briefly explain the policies., is Question 15 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	Prepared	Not Prepared
Number of Respondents	4	6

6.1 Four experts work in practical organizations, and these organizations have preparations for computer forensics.

6.2 Six experts work in non- practical organizations, and these organizations do not have preparations for computer forensic incidents. Two out of six experts who work in the university think that university does not have paramount needs for computer forensics.

7. In Taiwan, there indeed is on-the-job training for computer forensic investigators, and these training are mainly held without a fixed schedule. The teachers come from different sources although they are all computer forensic experts. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this program come from?, is Question 21 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	Yes	Do not familiar with this issue
Number of Respondents	6	4

7.1 Six experts say that there are on-the-job training programs for computer forensic investigators. Four of them say the on-the-job training programs are held irregularly. One states that on-the-job training programs are held annually in his organization. In addition, one state that the teachers come from senior investigators of MJIB or CIB. One says that the teachers come from suppliers of computer forensic tools or computer forensic experts.

7.2 Four experts do not familiar with this issue.

8. Training an investigator to become a computer forensic investigator at least needs one year. After that, a computer forensic investigator needs to update and to learn all the time. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?, is Question 23 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	High Standard	Continuous Training	Count by Years	Count by Months	Not Familiar with this issue
Number of Respondents	1	2	4	1	2

8.1 One expert thinks to train a computer forensic investigator should use high standards. However, this expert does not mention how long it takes to do so.

8.2 Two experts think that to train a computer forensic investigator is a continuous task due to the continuous changes of techniques.

8.3 Four experts think that to train a computer forensic investigator at least needs one year.

8.4 One expert thinks that to train a computer forensic investigator needs 2-3 months.

8.5 Two experts do not familiar with this issue.

9. The collision of hash function has influences on computer forensics. These influences may include: reliability of digital evidence, and more difficult to perform a computer forensic investigation. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?, is Question 25 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	Have Influences	Do not have Influences	Not Familiar with this issue
Number of Respondents	6	1	3

9.1 Six experts think that the collisions of hash functions have impacts on computer forensics. The possible impacts are 'the credibility of digital evidence' and 'more difficult to perform a computer forensic investigation'.

9.2 One expert does not think such impacts existed.

9.3 Three experts do not understand this issue.

10. In Taiwan, a computer forensic investigation reasonable encounters 0%-20% encrypted data. In the worst situation, a computer forensic investigation encounters at most 40% encrypted data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%, is Question 28 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinion	0%-20%	21%-40%	41%-60%	Not Familiar with this issue	No Opinion
Number of Respondents	4	1	1	3	1

10.1 Four experts, including two experts having practical experience, think the percentage of encrypted data situations is 0%-20%.

10.2 Based on his practical experience, one expert thinks the percentage of encrypted data situations is 21%-40%.

10.3 One expert thinks the percentage of encrypted data situations is 41%-60%.

10.4 Three experts do not understand this issue.

10.5 One expert does not provide opinion of this question.

11. In Taiwan, although the court cannot overlook the importance of digital evidence, the court normally give a low weighting to digital evidence. The only exception is that the digital evidence is valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, In your experience, do courts give a high or low weighting to digital evidence in your country?, is Question 35 in Round One questionnaire*.)**

According to the experts' opinions from Round One questionnaire, the conclusions are made in the table.

Opinions	High Weighting	Low Weighting	Depends on the Case
Number of Respondents	4	4	2

Opinions	High Acceptance	Low Acceptance	Depends on the Case
Number of Respondents	2	6	2

11.1 The number of experts choosing high weighting is the same as the number of experts choosing low weighting.

11.2 The number of experts choosing low acceptance is obviously more than the number of experts choosing high acceptance.

11.3 Two experts think that the weighting and acceptance of digital evidence are changed by cases. For example, the weighting and acceptance of digital evidence are very high in the computer crimes. On the contrary, the weighting and acceptance of digital evidence are relatively low in the traditional cases.

Appendix 8: The Results of First Round Questionnaire for Delphi Survey in Taiwan (Chinese Version)

Section 1: 數位鑑識(Computer Forensics)的情況

1. 依您所見，官方(政府)單位對於數位鑑識的觀點為? 您認為官方(政府)單位是否適當地重視此議題?

A. 政府單位隨著資安事件的頻繁發生，也深刻感受到數位鑑識的重要性，以國內目前的發展觀之，仍有待相關法令的建立、設備、鑑識實驗室與人才的擴充與訓練。特別是對數位鑑識人員應有的專業能力、相關經驗的培養及公正的、誠信的道德操守之嚴格訓練。

B. 隨著數位犯罪的增加，官方(政府)單位近年逐漸地重視。如法務部調查局和內政部警政署。最好能夠加強重視得能量。

C. 受到數位化環境的影響，官方(政府)單位必須重視此議題。現在算是一個好的開始。

D. 應速建立國家鑑識標準與程序。是的，官方(政府)單位是相當地重視。

E. 就我所知法務部調查局相當重視數位鑑識相關的議題，並已成立數位鑑識實驗室，希望能夠逐步協助提供法院可採信之數位證據。因此，官方(政府) 單位對於數位鑑識的觀點：能夠協助偵辦高科技（資訊）犯罪 。

F. 因應法庭活動所需，數位鑑識應重視此一問題。

G. 不重視。

H. 是的。算是一個好的開始。

I. 臺灣政府單位目前對於數位鑑識的認知，尚屬啟蒙階段，但是經過多方宣導發現數位鑑識對於犯罪調查確有幫助，因此已經開始擬定相關計畫與核撥經費與相關警政及犯罪調查單位從事有關數位鑑識之相關研究與應用。

J. 目前開始重視，算是起步。

2. 您對現今數位鑑識發展的看法? 您對於現況感到滿意嗎? 請簡單說明

A. 數位鑑識需要優秀的人才及設備，政府對於人才的培育及設備經費的投資相對是有限的，因此阻礙了這門科學的進展及應用。

B. 數位鑑識需要特殊的人才及設備，我國對於這方面算是剛起步。以現況來說僅有調查局及刑事局具備相關能力處理這類議題，尚不足以應付龐大的需求量。

C. 數位鑑識作業還缺乏許多標準的制定及相關工具的研發。

D. 仍在進行中，標準作業程序仍待加強，數位鑑識人員之訓練尚待加強。

E. 尚可，數位鑑識大多集中於少數人的認知中，並不向科學鑑識般廣為多數人所認知。相關的鑑識施行程序方法，也為建立一公認的標準或規範。就技術層面來看，相關的投入更是少。

F. 數位鑑識目前有刑事局及調查局設有專責單位，希望將來人員及設備能不斷擴充。

G. 現今數位鑑識在美國以色列等國家，有一定程度的發展。對現況趕到中等滿意，但在台灣似乎沒有特別在這一塊做研發，大多使用外國的工具。

H. 尚稱滿意，技術上持續發展，法界人士程度尚未提升。

I. 未填寫(無意見) 。

J. 現今數位鑑識的發展，還不是很明顯，在人才培育及經費支援上並加重。

3. 數位鑑識在貴國成立的年數(時間)有多久?

A. 在法務部調查局，刑事警局均有鑑識單位的設立，但有關數位鑑識是近幾年(4-5 年)才受到注意。刑事警察局電腦犯罪偵防小組是在民國八十五年九月份成立，八十八年七月擴編為偵查第九隊。

B. 大約四五年。

C. 未涉及。

D. 大約在四五年前開始推動。

E. 警政單位很早就認知此一議題，並有進修的警官，曾經從事此一議題的研究。最早的學術研究應為 2000 左右。而法務部調查局則於 2006 年成立全國首座數位鑑識專屬研究室（中心）。

F. 無資料可參。

G. 7.8 年。

H. 開始發展迄今，大約五年左右。

I. 本實驗室係台灣政府單位第一個公開設立有關數位鑑識的單位，成立時間為 2006 年 12 月 26 日，目前大約只有半年時間，民間部分有關數位鑑識的部分，不得而知。

J. 最近二年才有此共識。

4. 數位鑑識在貴國算是熱門的議題嗎?

A. 應該是大家都認為重要，但並非主流的熱門議題。

B. 不算是非常熱門。

C. 不算是熱門的議題。

D. 不算是非常熱門。

E. 就目前的學術研究而言，算得上熱門的議題。

F. 學界對此討論議題甚多。

G. 目前在資安界算中等。

H. 否。

I. 目前算是新興議題，但還談不上熱門，因為有關數位鑑識工作的成效還沒有被政府單位及民眾所廣泛熟悉。

J. 並不算。

Section 2: 數位鑑識的步驟

5. 依您所見，在貴國執行數位鑑識時可以依循的標準程序(Standard Operation Procedure)為何?

A. 準備工作(Preparation)、紀錄與文件化（Documentation）、收集（Collection）、驗證（Authentication）、分析（Analysis）、保護（Preservation）、產出結果（Production）、報告文件（Reporting）八種程序。

B. 本人於 2003 年始推倡 SOPs 的建立，但是目前沒有一個統一的標準。

C. 未涉及。

D. 一般而言是一林宜隆教授所提出與美國所用之程序。

E. 目前為有官方的標準程序，但普遍採用一些警政單位依循的蒐證原則。同時有多的政府單位及研究單位進行制訂與發展於特定的數位鑑識工作進行時之標準程序。目前所知，法務部調查局應陸續制訂相關標準程序中。

F. 非本人業務範圍。

G. 刑事局有一套數位鑑識應注意事項：警察偵查犯罪規範係依據刑事訴訟法等規定，綜合有關偵辦刑事案件規定訂定之，作為辦案程序之準據。在第六章第十四節第二項偵辦電腦犯罪案件，如有需要得請求各直轄市、縣（市）警察局刑警（大）隊電腦犯罪偵防小組協助偵辦；涉及系統入侵、網路洗錢等重大案件得會同刑事警察局資訊室電腦犯罪偵防小組協助偵辦。該規範第六章第十四節中列出了有關執行電腦犯罪案件搜索前置作業、執行電腦搜索、電腦犯罪案件證物處理、電腦犯罪案件電腦鑑識等應注意事項。調查局也有建構相關的數位證據程序 。

H. 搜集→採證→分析→報告→法庭呈現。

I. 目前台灣有關數位鑑識並未有統一之標準作業程序(SOPs)，而 SOPs 之訂定與執行，必須與國情之法律相符，因此目前仍參考歐美等國家有關數位鑑識之相關 SOPs，並依實際執行時之狀況，進行修正。

J. 目前並未有可依循之 SOPs。要各自設定。

6. 您對於數位鑑識標準程序(SOPs)之重要性的看法?

A. 數位證據的重點在於其呈現於法庭時所具有的證據能力，因此對於數位證據的處理沒有標準程序，個人認為很難在法庭上發揮證據能力。

B. 非常重要,數位鑑識標準程序是建立數位證據之證據能力及證明力的關鍵。

C. 有了「數位鑑識標準程序」才能確保鑑識的結果是一致、完整且正確的。

D. 非常重要,因為對電腦犯罪之刑事鑑定具有重大意義。

E. 標準程序(SOPs)不只讓數位鑑識的工作更具效率及避免出錯。也讓數位鑑識產出的成果能夠其他公正單位進行檢驗，也更具公信力及讓產出的數位證據更具證據能力。

F. 在法庭活動時可以讓法官及當事人對數位鑑識過程能有檢驗之標準。

G. 對於證據的證據能力上面，數位鑑識標準程序(SOPs)，是非常重要的。

H. 作為數位證據真實性之基礎。

I. 我認為數位鑑識標準程序(SOPs)對於數位鑑識之重要性在於對數位證據的完整性、不可否認性及重現性的確保，因為 SOPs 的訂定與執行，使數位證據呈現的結果，可接受公評。

J. 十分重要。

7. 據您所知，是否有條文規範數位證據(digital evidence)在開庭過後需要保存多久時間? 如果有，期限為?

A. 對於數位證據的保存期限，目前沒有明確指出需保存多久，一般案件結束之後，除非有後續的訴訟動作，否則數位證據就應該要歸檔保存。個人認為所有的鑑識報告，應至少保存三年，惟涉及刑事案件之鑑識結果，最好是永久保存。

B. 目前應該是沒有明確規範。

C. 未涉及。

D. 這一點並不清楚。

E. 不知。目前應該是沒有，而是依循一般證據的保存規定。

F. 沒有規定。

G. 不清楚。

H. 案件結束。之後並無規範。

I. 我個人在美國參訪有關的數位鑑識實驗室，發現他們對於數位證據的保存除了訴訟正在進行尚未結案的部分外，另外對於已經結案的部分最少都會保存 5 年以上的時間。台灣則無相關規定。

J. 目前尚未明訂。

Section 3: 數位鑑識的特徵

8. 據您所知，數位證據的主要特性是什麼? (例如: 一致性(Integrity))

A. 數位證據具高度揮發性、易於被更改且可被完美複製、蒐集到的證據會因處理過程而被改變、電腦原始資料不具可讀性、資料量可能極大、電腦資料無法個體化等特徵。

B. 不具可讀性，易遭破壞性, 原始作者不易確定，可複製性，具有中介資料。

C. 應具備一致性、完整性。

D. 資料之一致性, 易遭破壞性, 完整性與證據能力。

E. 易竄改、不易取得、不易呈現為一般人所認知、具備證據能力

F. 數位證據一致性(同一性)的討論應該是在證據能力及證據力進行討論。就數位證據本身之特性主要有作者不易確定

G. 可無限無差異複製、不易銷毀、原始作者不易確定、資料完整性驗證。

H. 易遭竄改性、可復原性。

I. 數位證據的主要特性我個人認為如下，脆弱性、易複製性、一致性及多樣性等特性。

J. 不可否定性。

9. 從數位鑑識的觀點來說，您怎麼看待數位證據中所呈現的中介資料(meta-data)?

A. 電腦鑑識人員必須注意下列三項數位證據原則：在不改變或破壞證物情況下取得原始證物;證明所鑑識之證物來自原扣押證物並與之相同;在不改變證物情況下進行鑑識分析。

B. 為數位證據的特色之一，是一般物理證據所不能提供的。

C. 數位鑑識作業的過程可能需要產生「中介資料」。

D. Meta-data 是一個引導呈獻數據之資料, 也是數位件事成功與否之關鍵因素之一。

E. 未填寫(無意見)。

F. 非本人專業。

G. 必須有一定公信力的軟體，作為 meta-data。

H. 不了解問題。

I. Meta-data 對於數位鑑識而言是相當有用的資料，因為檔案開發者及利用者對於各種檔案格式會留下這些所謂的 meta-data，而一般 user 對於 Meta-data 並不了解，因此這些 meta-data 就成為相當重要的數位證據。

J. 可作有力參考。

10. 您認為數位證據中所呈現的中介資料的可信度(trustworthiness)為何?

A. 不同來源其品質控制與可信度也有所不同。

B. 透過具有公信力的數位鑑識工具，其可信度不是問題。

C. 中介資料的可信度受到相關工具的影響。

D. 應是可信的, 除非是有箇中高手入侵系統加以篡改。

E. 未填寫(無意見) 。

F. 非本人專業。

G. 可信度隨著鑑識者有充分足夠的能力去證明他的程序正確性，資料的完整性。

H. 不了解問題。

I. 我認為 meta-data 的產生主要是依照檔案格式設計者的想法所設計出來的，一般除非對於檔案格式相當精通了解，否則很難去偽造及變造 meta-data，因此 meta-data 的可信度應該是相當高。

J. 尚可。

11. 您認為資訊安全(computer security)跟數位鑑識(computer forensics)兩者之間的關係為何?

A. 數位鑑識是讓資訊安全事件還原的一項重要工作，也是遏阻資訊安全事件發生的方法之一。

B. 資訊安全的目的在於防範，而數位鑑識的目的在於還原受害端的蒐證。兩者並無直接關聯，但是藉由數位鑑識可以強化資安能量。

C. 從數位鑑識作業可以提出資訊安全的改善能力。

D. 資訊安全是指如何保護資料, 使其不為其他人得知其內容之措施, 數位鑑識則是要還原受害端如何受害之原貌。

E. 數位建議一般被定位為事後調查，而吾人認為數位鑑識除了協助事後的調查外，用於安全測試及資安稽核也是可行的。整體來說，資訊安全的範圍應包含數位鑑識。

F. 非本人專業。

G. 兩個是有交集，例如發生資安入侵事件需要鑑識人員，透過鑑識工具研發，可以找到系統的一些漏洞。

H. 數位鑑識有兩種，一種是發現問題之數位鑑識，一種是法庭攻防之數位鑑識，均屬資安事件發生後的後階段程序。

I. 資訊安全如果做的完全，那麼就可留下許多有用的數位證據以供追查，例如網路系統的稽核紀錄(security log)，因此資訊安全與數位鑑識的關係是相輔相乘的，有完善的資訊安全對於數位鑑識的結果將有極大之助益。

J. 數位鑑識是資訊安全的驗證並推動能量 。

12. 當執行數位鑑識的調查時，您認為需不需要了解被調查者的背景? (例如：有幾隻狗? 開什麼車? 有什麼興趣?) 還是專注於分析數位資料? 請簡述原因

A. 個人背景會影響其犯罪動機及行為習慣，實際上是有高度的關連性，因此需要了解被調查者的背景，而不只是專注於分析數位資料。

B. 需要。如此一來，將可能獲得一些數位資料所不能給予的資訊 (例如：密碼) 。

C. 了解被調查者的背景，可以協助數位鑑識的調查方向。

D. 需要了解被調查者的背景, 因為從這一些背景常可看出一些和犯罪有關之蛛絲馬跡, 之後再專注於分析數位資料。

E. 有兩種不一樣的觀點，調查者應專注於分析數位資料，指出事件的關連。另一種觀點為調查者應了解被調查者的背景，以便於重組事件。我認為後者更能協助執行數位鑑識的調查時還原事件過程。

F. 鑑定人之專業背景當然需要瞭解，可以增加該份鑑定報告之證據力。

G. 被調查者的背景，是犯罪偵察中非常重要的一部份，一定需要瞭解。

H. 沒意見。

I. 我認為如果有一些案件的背景資料，將有助於對數位資料的解析，因為只單純的分析資料，並不會知道如何分析出真正與案情有關的數位證據，例如要求送鑑單位提供關鍵字的意義，就是期望由關鍵字中稍稍了解案件的性質與背景。

J. 不是很需要，但有時有幫助於瞭解狀況。沒有，應不致於影響結果。

Section 4: 數位鑑識的組織

13. 貴國執法體系中數位鑑識單位的層級是高於一般警局? 還是等於? 還是低於?

A. 主要的數位鑑識單位是設於刑事警察局，是屬警察體系的專責機構。但另外在法務部調查局也有類是單位。

B. 高於一般警局。

C. 高於一般警局。

D. 據我所知是高於一般警局。

E. 應為等於。

F. 我國數位鑑識專責單位分別為內政部刑事警察局及法務部調查局。

G. 是隸屬在警察局裡，低於。

H. 屬於調查局(三級行政單位)內之資訊室下屬單位。

I. 以本局為例，本局的數位鑑識實驗室層級是高於一般警局，因為是設在局本部，而不是一般的地區單位，至於警方體系有關數位鑑識單位的層級，

無法判斷，因為分屬不同單位。

J. 低於。

14. 貴國的執法單位有將數位鑑識進行委外處理嗎?

A. 數位鑑識在台灣並沒有非常知名的商業公司提供此服務，因此執法單位對於數位鑑識工作仍然以公務機關自已執行為主。

B. 目前並沒有。

C. 沒有。

D. 尚未聽說。

E. 就我所知，目前無。但在規劃進行中。

F. 無資料可參。

G. 大多自己處理。

H. 本局有資安鑑識實驗室，但若有特殊情況，仍會與其他廠商合作。

I. 就我所知美國執法單位的數位鑑識工作除了有正式職位的警察及調查員從事數位鑑識作業外，另外還有招募民間人員從事數位鑑識工作，我國目前對於數位鑑識工作仍未委外處理，全部由專業司法人員負責。

J. 應還沒有。

15. 您的工作單位對於數位鑑識是否有所準備? 如果有，請您提供貴單位的名稱。 同時，請您簡單說明這些政策。

A. 本人在學校服務，因此工作單位對於數位鑑識沒有急切相關的必要性。

B. 本人在學校服務，目前並沒有。但正在規劃數位鑑識中心。

C. 沒有。

D. 目前並沒有, 因資料並不是重要到一定要完全加以保護。

E. 有，成大資通安全研發中心。協助進行資安事件的分析並重新事件過程。提供資訊分析技術。

F. 無。

G. 沒有。

H. 調查局。2006 年 12 月成立資安鑑識實驗室。

I. 本局對於數位鑑識已經實務在運作中，法務部調查局資安鑑識實驗室。

J. 有。法務部調查局。本局政策是十分支持數位鑑識工作。

16. 在貴國， ”資訊安全的議題” 和 ”數位鑑識的議題” 是否由不同的單位來處理？如果是，請您說明貴國 ”資訊安全的單位” 跟 ”數位鑑識的單位” 兩者之間的關係為何?

A. 資訊安全與數位鑑識是隸屬於不同的單位，兩單位之間應有合作的關係。

B. 是的。目前的關係是合作，因為數位鑑識畢竟性質較特殊，並不是每個單位都瞭解。

C. 是

D. 資訊安全的議題和數位鑑識的議題因權責不同, 而是分屬不同單位處理。

E. 資訊安全的議題由較高的層級，組成跨部會的單位處理。數位鑑識的單位議題由警政單位及調查單位處理。為上下層級關係，但不直接管轄。

F. 就我理解，刑事偵查機關同時負責資訊安全及數位鑑識，以刑事偵查機關而言，未有以兩者作區分之專責單位。

G. 兩個單位差不多。

H. 是的。數位鑑識屬於犯罪防制的單位，資訊安全則否。

I. 在本局有關資安與數位鑑識是都是由資訊部門負責，但仍有細分為 2 個不同單位負責。

J. 由不同單位處理。資訊安全的單位是著重於安全維護，數位鑑識的單位著重於取得行為證據。

Section 5: 數位鑑識的的認證

17. 貴國的數位鑑識專家是如何形成的? 是透過何種測驗? 或是透過何種步驟?

A. 目前國內有關數位鑑識領域仍然有很大的改進空間，目前並沒有政府機關舉辦數位鑑識專家認證考試。

B. 受訓或經由實戰磨練。目前並無一個統一的標準可以依循。例如 Association of Computer Investigative Specialists (IACIS) or TWCERT/CC。

C. 未涉及。

D. 受鑑識專業訓練, 例如, 警察大學或警專, 致於是透過何種步驟則不甚清楚。

E. 目前已取得國外（美國或英國）認證為主。

F. 無資料可參。

G. 目前國內有 TWCERT/CC 提供這項認證，上完他們的課，並且繳交作業，參加考試。

H. 受訓或參與認證，經由實驗不斷磨練。

I. 目前本局從事數位鑑識人員都是由從事調查工作但具資訊專長的人員來選拔，並接受相關數位鑑識訓練而形成的。

J. 受訓及工作經驗。

18. 貴國是否接受他國的數位鑑識專家前來從事相關工作?

A. 應該有邀請他國數位鑑識專家前來交流，至於正式工作我認為應該沒有。

B. 若有應當會接受，但目前沒有。

C. 是。

D. 是的，例如，委請李昌鈺博士鑑定，或送美國加拿大相關單位鑑識之。

E. 應為接受，但目前沒有實例。

F. 鑑識人員無國籍限制。

G. 接受。

H. 目前尚無。

I. 目前政府相關法令並未有此規定，因此無法接受。

J. 不接受。

19. 貴國是否有 ”某個單位” 對於數位鑑識專家進行認證? 如果有，此單位的名稱為? 所依循的標準為何?

A. 沒有。

B. 沒有。

C. 未涉及。

D. 目前據我所知是沒有，電腦技能基金會可能會有，但其為民間單位。

E. 無。

F. 無資料可參。

G. 國內有 TWCERT/CC 提供這項認證，上完他們的課，並且繳交作業，參加考試。依造 TWCERT/CC 自己的標準。

H. 無。

I. 目前我國並未有此單位可對數位鑑識專家進行認證。

J. 無。

Section 6: 數位鑑識專家的訓練

20. 政府相關部門是否願意舉辦活動支持數位鑑識從業人員的教育 or 訓練? 是否支持數位鑑識的研究? 請您簡單說明政府相關部門是如何支持這類活動。

A. 近年來，中央警察大學、鑑識科學學會、刑事局及法醫研究所等單位，均積極辦理各種學術研討會，提供鑑識人員在職訓練及經驗交流的管道，提升國內刑事鑑識水準。

B. 警察大學和調查局都有舉辦各類研討會，藉以提升從業人員水準。

C. 未涉及。

D. 是的，例如經常補助學校(例如中央警察大學)舉辦數位鑑識等之研討會，以擴展相關人員知識與經驗交流。

E. 警政與調查局等執法單位或多或少進行支持，包含支持研究計畫及舉辦研討會或 workshop。

F. 政府很重視數位鑑識之發展，學者正大力促成數位鑑識實驗室之建立。

G. 讓數位鑑識從業人員，參與廠商的課程，或是一些機構的認證課程。

H. 是。送至國外接受訓練，編列預算進行技術與法制層面之研究。

I. 目前我國政府對於數位鑑識人員的教育及訓練相當支持，因此每年編列許多教育訓練費用以供數位鑑識人員增進數位鑑識方面的本質學能。

J. 目前我只知道本局有此常態性訓練活動。

21. 就您所知，貴國有提供數位鑑識調查員的在職訓練嗎? 通常多久舉辦一次? 師資來源為?

A. 數位鑑識調查員的在職訓練主要以研習會或學術研討會的方式不定期進行，師資來源主要是以大學相關領域教授及刑事局與調查局之資深專業人員擔任。另外也有由國外合作機構提供相關教育訓練，例如 EnCASE 教育訓練。

B. 研討會以及國外訓練。不定期。

C. 未涉及。

D. 數位鑑識調查員的在職訓練應該是有，只是僅參與一次，其後便不知是否持續進行。

E. 不知。

F. 無資料可參。

G. 不清楚。

H. 有。不定期，大都為國外訓練。

I. 目前本局有關數位鑑識人員的在職訓練大部分為邀請國內外從事數位鑑識相當專業的廠商或是專業人員來授課。訓練舉辦期間不定。

J. 本局會作，每年一次。

22. 貴國有沒有訓練數位鑑識專家的方法? 如果有，請您簡述之

A. 目前國內並沒有標準訓練數位鑑識專家的方法，除了 TWCERT/CC 曾經開過電腦鑑識的訓練課程。因此業務主管機關如刑事局及法務部調查局應是選送優秀人員參與國外訓練課程培養相關技術。

B. 有 (例如 TWCERT/CC)。但是一樣不具備強制性亦不是唯一的選擇。

C. 未涉及。

D. 有, 政府單位曾委請警察大學林宜隆教授規劃之。

E. 不知。

F. 無資料可參。

G. 就我所知為 TWCERT/CC 的數位鑑識認證班。

H. 國外受訓。

I. 目前都是將具有資訊專長的調查人員直接送到國外相關之鑑識組織或是找尋相關之鑑識課程來培養訓練。

J. 派員受訓，並參加國外測驗。

23. 根據貴國數位鑑識發展的現況，您認為訓練依各數位鑑識調查員所需的時間是多久?

A. 個人認為數位鑑識是一項高度知識密集的工作。數位鑑識專家的識能，必須涵蓋作業系統、網路、軟硬體設施、數位鑑識作業程序及法律議題，因此訓練課程必須針對已經具備基礎的人員，而訓練時數及實作時數必須採高規格、高標準，數位鑑識專家的培訓可透過專業證照制度來完成。

B. 這是一份複雜的工作。保守估計約需 1~2 年。

C. 未涉及。

D. 仍持續發展中，數位鑑識調查員所需的訓練時間不一而足， 應是長時間持續地，以面對駭客或入侵者持續不斷精進之入侵技巧。

E. 約需 1~2 年養成為具備基本能力的數位鑑識調查員。

F. 數位科技領域浩瀚，發展迅速，需要不斷地訓練。

G. 2-3 個月。

H. 沒計算過。

I. 我個人認為一個真正可用的數位鑑識人員的訓練時間最少需要一年，最佳的時間是 3 年。

J. 要一年。

Section 7: 數位鑑識專家的技巧

24. 在數位鑑識的領域中，您對於雜湊函數(hash function)的重要性有何看法?

A. 雜湊函數對於數位證據的保存有相當重要的意義，防止數位證據遭受竄改之疑慮。

B. 相當重要，確認數位證據的拷貝版和原版之間的關係。

C. 未涉及。

D. 雜湊函數(hash function)可以加密資料，用以保護資料被串改或竊取。

E. 相當重要的程序多用以作為證據的驗證。但大多數未考慮雜湊函數(hash function)碰撞的問題。僅有少數考慮所謂的 perfect hash。

F. 減少數位證據同一性及真實性遭受爭執。

G. 可以驗證資料是否是同一份資料。

H. 驗證數位證據之真實性，但此真實性是指採集證據後，進行分析，到製作報告與法庭呈現時，這一個流程的真實性。並非指此一數位證據未曾遭到他人之竄改。

I. HASH 可以用來幫助檔案的完整性及一致性，因此在數位鑑識中，HASH 是必備程序。

J. 有其重要性，避免資料被竄改。

25. 某些雜湊函數的碰撞已經被證實(例如 MD4, MD5, and SHA0)，您認為雜湊函數的碰撞對於數位鑑識有什麼影響?

A. 雜湊函數的碰撞對於數位鑑識而言表示數位證據會有偽造及竄改之可能，因此其證據能力會受到質疑。

B. 增加數位鑑識的難度，費時費力 (例如 用多個 hash 去驗證) 。

C. 未涉及。

D. 這是數學一對一與一對多之問題, 尤其是後者在還原成原始資料時, 會無法得知原始資料是哪一個。

E. 一旦用以驗證的雜湊函數產生碰撞問題，則數位證據可能會被推翻。但就目前現況而言，要產生此一情況，可能還有一段時間。況且未來所採用的 hash bit 長度愈長，則碰撞欲難達行。但未來利用 perfect hash function 才是解決的方法。

F. 非本人專業，無法回答。

G. 會對他是否為同一份資料有疑惑，但是碰撞的機率是非常低的，可以多用幾種 hash，去驗證。

H. 不瞭解。

I. 目前部份的 HASH 函數發生碰撞情形，對於數位證據的完整性及一致性當然有一定程度之影響，會影響數位證據的可信度，可信度會降低。

J. 沒有。

26. 就您所知，以數位鑑識的觀點來看，對於雜湊函數的碰撞有什麼對策?

A. MD5 及 SHA-1 已經被破解，因此必須使用更安全的 SHA-224、SHA-256、SHA-384 及 SHA-512 的密碼系统，以保障資料的安全性。

B. 用多個 hash 去驗證。

C. 未涉及。

D. 處理原始資料前，須先確定過慮原始資料的方法。

E. perfect hash function。

F. 非本人專業，無法回答。

G. 多用幾種 hash，去驗證。

H. 不瞭解。

I. 期望密碼學者能開發出新的 Hash Function，以維護數位證據的完整性及一致性。

J. 用多種方式。

Section 8: 數位鑑識的瓶頸

27. 就您所知，貴國的數位鑑識調查行動是否有遭遇到由時戳(time-stamp) 所以起的困擾? or 遭遇到由不同時區(different time zones)所以起的困擾? 如果有，您習慣如何處理這類問題?

A. 電腦網路 log 資料會因為不同時區(different time zones)所引起的困擾，因此可以運用網際網路工程技術組(IETF)與美國國家標準技術院(NIST)都制定有的時戳服務，以具備準確時間公信力的時戳服務中心(TSA)擔當電子世界裡時戳為憑的角色，以克服 time-stamp 及 different time zones 的問題。

B. 台灣並沒有跨時區的問題。而且"時間"對於數位鑑識是相當重要的，這是數位鑑識人員的基本工作。

C. 未涉及。

D. 以本地收到資料或被攻擊之時間為準, 因此不會有困擾。

E. 大多時戳(time-stamp)或不同時區(different time zones)所引起的問題，於受相關教育訓練時應已提供相關的解決方法。就我所知，大部分均無此一問題。利用對照及轉換均可處理這類問題。

F. 尚未遇過此類問題。

G. 尋找他的網路區段，倒到他所在位置，與時間作比照。

H. 我不認為時戳和時區是個問題。實務上網路電腦犯罪之調查，時間的確認是非常重要也是最基本的工夫。至於電腦鑑識方面，僅能強化現場紀錄工作。未來發展還需要多參照國外經驗。

I. 目前對於 time-stamp 的利用尚不普遍，所以並未有困擾，至於時區的問題更小，因為我國只有一個時區。時區問題的處理可由鑑識軟體的時區校正功能來設定解決。

J. 還沒有。

28. 就您所知，貴國數位鑑識調查行動所遭遇到的加密資料其百分比為何?

(1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%

A. 依據個人認知，目前國內數位鑑識調查行動中遭遇加密資料其百分比並不是很高，因此個人認為在 0%~20%間。

B. 0%-20%。

C. 未涉及。

D. 未曾實際參與鑑識工作, 因此無法得知。

E. 未填寫 (無意見) 。

F. 無數據可參。

G. 41%-60%。

H. 0%-20%。

I. 就我個人進行鑑識的案件，發現檔案加密的部分比例為（21%-40%）。

J. 0%-20%。

29. 就您所知，貴國的數位鑑識調查員如何處理加密的資料?

A. 運用相關工具進行解密的嘗試。

B. 1. 試圖解密 2. 轉而使用其他證據。

C. 未涉及。

D. 設法破解之, 否則便從他處佐證以繼續鑑識工作。

E. 未填寫 (無意見) 。

F. 非本人專業，無法回答。

G. 使用解密軟體。

H. 詢問當事人、暴力破解法等，並沒有採取美國取得搜索令，安裝 keylogger 的方式。

I. 利用業界功能比較強或較普遍的解密軟體，將加密資料予以解開，另外對

於使用自行開發或使用特殊的加密演算法之加密資料，則需藉助特殊管道協助。

J. 破密。

30. 就您所知，貴國的數位鑑識調查行動是否有遭遇任何困難? 請您簡單條列

A. 1.基層鑑識人員缺乏足夠的數位鑑識能力, 2.執法機關應擁有相同的數位鑑識專業素養, 3.資通安全鑑識實驗室軟硬體設備之加強, 4.網路跨國犯罪的問題，追查所遭遇的困難

B. 人員缺乏、訓練不足、工具的不足

C. 受到專門技術人員、標準作業程序、工具的使用等多方面的影響

D. 最主要是受害單位鑑於顏面與商業上之利益, 皆不願聲張, 不報案

E. 1.新技術推陳出新。2.未能有數位特徵相關的資料庫可供比對。

F. 大型資料庫之資料解讀、扣案

G. 工具的不足，包含硬體、軟體，資料難以回復

H. 第一線偵查人員對於數位鑑識之不瞭解。數位鑑識較為耗時，且扣押物品難以確定，若電腦眾多，如何扣押也是問題

I. 目前有關數位鑑識調查最困難之部分在於對於龐大企業的數位證據的擷取，由於存放數位證據設備的規模與種類龐雜，因此對於此類型之數位鑑識工作感到相當困難

J. 技術與設備不足。資料量太大

31. “技術” 和 “人” 是兩各不同的層面。單純檢驗電腦上的濫用是簡單的，然而

如何證明嫌疑犯就是濫用電腦的人則相對困難。就您所知，貴國的數位鑑識調查員是如何處理這類的問題?

A. 一般機關中個人對於系統的使用權限是有管制的，因此從電腦紀錄檔及權限控管機制去追蹤使用者濫用的情形。

B. 配合傳統的犯罪偵查的方法 (例如 監視錄影) 。

C. 未涉及。

D. 這方面卻有困難, 只是從錄影從 IP 從追蹤系統確可追查到犯罪者。

E. 大多利用案件偵辦或傳統的犯罪偵察的方法，而非全部利用數位鑑識方法。多數數的數位鑑識調查員也會配合具有偵察權之人員進行調查工作。

F. 本人非數位鑑識調查人員，無法回答專業問題，不過數位證據真實性遭受質疑時，仍可就其他證據資料進行調查。

G. 利用其他資料作為主要證據，例如網路詐欺，一定要去提錢，跟這些證物做交叉比對。

H. 此一問題並非鑑識人員職掌之範疇，已經屬於法庭審理過程，對於數位證據、其他事證與環境證據整合起來，經由經驗法則、自由心證，將片段事實還原可能之現場重建。

I. 如何証據嫌犯就是電腦使用人，有兩種方式，第一個是針對電腦內的資料進行分析比對，例如照片等等，另外就是針對送鑑的數位證物，進行例如指紋及 DNA 的分析工作等等。然而，我認為這個問題已經不屬於我的工作範圍。

J. 由檢察官去查問。我們只呈現所看到的。

Section 9: 數位鑑識的交流

32. 就您所知，貴國的數位鑑識組織是否有跟國際的相關組織做交流? 如果有，請問交流的方式為何?

A. 1. 派員參觀訪問, 2. 參加教育訊練課程, 3. 參加研討會, and 4. 建立合作關係

B. 參加研討會、派員赴國外考察與研究。

C. 未涉及。

D. 有，調查單位常派員赴國外考察與研究，也會邀國外鑑識專家來台訪問與指導。

E. 目前所知，與國外交流多為參訪或邀請至國內進行專題演講，實際合作方式不得而知。

F. 舉辦研討會。

G. 研討會，去國外參訪，受訓。

H. 有。參加研討會、互訪。

I. 本局資安鑑識實驗室目前每年定期有派員至美國 IACIS 組織受訓即加入成為會員，另外對於多個知名的鑑識組織亦有所接觸。

J. 參觀訪問，邀請演講。

33. 就您所知，貴國的數位鑑識組織/學者是否有與貴國的相關數位鑑識組織/學者做交流? 如果有，請問交流的方式為何?

A. 1. 邀請演講或授課, 2. 技術指導, 3. 顧問工作, and 4. 舉辦研討會

B. 參加研討會以及成為顧問。

C. 未涉及。

D. 答案與上一題相同。

E. 多為合作進行研究計畫。

F. 舉辦研討會。

G. 研究案，研討會。

H. 有，聘做顧問、參加研討會。

I. 交流的方式應該係採舉行會議或召開論壇的方式來進行。

J. 高峰論壇方式，參訪。

34. 就您所知，數位鑑識這方面的工作人才通常將其專業經驗與何人交流?

(1)同事 (2)長官 (3)其他(請說明)

A. 同事或長官應該都有交流。

B. 同事。

C. (1)同事 (2)長官。

D. 定期之研討會中可與他人交換經驗與知識。

E. 同事、其他相關學者或技術人員。

F. 依案件需要所接觸到之人士。

G. (1)同事 (2)長官以及網路上從事相關活動之人。

H. 同事、企業人才(科技發展迅速，數位鑑識必須具備各種高科技知識) 。

I. 我個人會將我的專業經驗與同事交流，另外有時會將個人的專業經驗與其他單位從事數位鑑識人員進行意見交換。

J. 同事。

Section 10:法庭對數位鑑識的觀點

35. 以您的經驗，法庭對於數位證據的重視度(採性度)是高? 是低?

A. 高

B. 整體而言是'低'。 數位證據並不完全被法律人所了解

C. 低

D. 目前是高度重視的，只是數位證據因易遭竄改，在法庭上不一定會受到法官之青睞與採信

E. 重視度高，但是實際採用比率仍不高。

F. 數位證據當然是證據資料之一種　依案件需要而定 (要修改)

G. 目前是低的，大多作為輔助證據

H. 低，法律人不太瞭解資訊科技。

I. 就我個人經驗，法庭對於數位證據的認定應該是看案件性質而定，如果係電腦犯罪，則有關犯罪的數位證據的重視度應該是相當高，相對的，如果是一般刑事犯罪，則數位證據的採性度則應該較低

J. 算是高

36. 就您所知，在法庭上使用數位證據是否有遭遇任何困難? 如果有，造成這情形的主要原因為?

A. 為了使由電腦系統中取出的數位證據能為法庭上所認可，必須要避免或降低其易竄改或消失等特性，並已可信賴的形式保存，才能使數位證據為法律、法庭上所認可成為判決的依據。因此需要透過一定的程序與原則來達

成數位證據的擷取、分析、解讀的過程，以利事件的偵查及使數位證據作為法庭上的證供。

B. 數位證據並不完全被法律人所了解。

C. 有。

D. 目前是高度重視的，只是數位證據因易遭竄改，在法庭上不一定會受到法官之青睞與採信。

E. 主要為審判者或審理者對數位證據的可信度及公正性有質疑，未能完全採信。

F. 因為法院都為法律背景人士，較少資訊人才，因此數位證據之勘驗、調查往往耗時耗力，需要花時間在基礎觀念建立以說服法官。

G. 案例還不夠多。法官檢察官不瞭解數位證據。

H. 不懂數位證據之特性。

I. 因為數位證據的多樣性，所以有時要呈現數位證據可能需要藉助一些設備才能顯現，目前本國法庭上有關數位證據的審理仍偏向於靜態的展示，故應該還沒有困難，如果改為動態方式，則可能有困難。

J. 呈現方式，解釋說明，沒有基本觀念。

37. 就您所知，在貴國嫌疑犯是否有義務提供數位證據? 貴國是否有哪一部法律有規範這樣的義務? 如果有，那部法律的名稱是?

A. 我的認知目前嫌疑犯沒有義務提供數位證據。

B. 沒有。

C. 未涉及。

D. 嫌疑犯爲自己之清白當然願意提供數位證據，只是若對當事人不利時，自然不會提供，至於是否有律法規定則不得而知。

E. 應無規定嫌疑犯有義務提供數位證據。但是，嫌疑犯可作舉證，不確定是否包含數位證據。

F. 我國被告不負舉證義務，依我國刑事訴訟法，舉證義務在檢方。

G. 沒有。

H. 舉證責任誰負擔的問題，而非是否有義務提供。若有舉證責任，則當然必須舉證，不論是否屬於數位證據。民事訴訟法、刑事訴訟法目前尚無此規定。

I. 我國目前並未要求嫌犯有提供數位證據的義務，但就我所知，嫌犯可以就對於個人有利證據的部分提出說明，所以包含數位證據。

J. 不知。

38. 就您所知，貴國是否有現行法律跟不上數位鑑識的發展之現象？如果有，這是否影響數位鑑識調查員的辦案態度？如果有，請簡述

A. 現有法律對於網路世界的犯罪行為而言似乎永遠是落後的，因此個人認為應該會影響數位鑑識調查員的辦案態度，因為他們沒有完善的法律可以遵循，所以會陷入工作的判別困難，及喪失積極追查的心態。

B. 有。可能導致鑑識調查員不積極偵辦。

C. 有。數位證據不被採納。

D. 應不會，在法庭上任何有利之證據皆是有效的，是否是數位證據則不是很重要

E. 有此一現象。

F. 有。因為案件辯護人鮮少針對數位證據鑑識進行爭執，法院亦很少對數位證據適法性問題表示明確意見，未見實務因數位證據鑑識程序不嚴謹導致案件有徹底失敗，因此在法規面上未有很深之著力。

G. 有，但必須用現有法律去規範。

H. 有。美國在 2006 年 12 月 1 日，修正通過民事訴訟法有關數位採證之部分，對於數位採證之舉證責任、程序都有很大的演進，我國目前法令仍無法解決許多細節性的問題，例如民事案件中，若提供數位證據費用過鉅。則該由何人負擔。

I. 台灣數位鑑識的發展尚屬萌芽階段，因此法律上有關數位證據及數位鑑識的部分仍須修訂，對於我們這些從事數位鑑識工作的人員確有影響。

J. 還沒有。

Section 11: 數位鑑識專家的工作習性

39. 身為數位鑑識專家，在工作上對於不必要的資料，您是否會使用資料清除工具?

A. 我會使用資料清除工具。

B. 會。

C. 不會。

D. 局部會, 因一一清除除耗費時間耗費人力, 除非電腦速度變慢了。

E. 會。

F. 會。

G. 不常。

H. 不懂。

I. 會的，會使用 wipe 工具來進行資料之清除工作。

J. 會。

40. 身為數位鑑識專家，對於工作上的資料，您是否會使用加密工具?

A. 我會使用加密工具，例如 PGP 工具。

B. 會。

C. 不會。

D. 重要資料一定加密，只是加密並非萬靈丹，必須隨時留意資料有洩密之疑慮否。

E. 會。

F. 會，使用文書軟體本身之加密功能。

G. 會。

H. 不一定。

I. 大部分會，但有時也會稍稍偷懶，因為密碼的記憶工作是一項困難的事。

J. 會，看需要。

Appendix 9: The Results of First Round Questionnaire for Delphi Survey in Taiwan (English Translation)

Section 1: Conditions of Computer Forensics

1. From your point of view, what is your government's perspective on computer forensic issues? Do you think the emphasis they put on it is currently at an appropriate level?

   A. With the increasing number of cyber crimes, government deeply realizes the importance of the computer forensics. The urgent needs of computer forensics are: legislating the relevant law, training the computer forensic investigators, recruiting manpower for computer forensics, purchasing the latest equipments, building the computer forensic laboratories. Most important of all, the morality and the ethics of the computer forensic investigators should be concerned seriously as well.
   B. With the growth of the cyber crimes, government agencies start to put emphasis on these issues recent years. The government agencies include MJIB, and *National Police Agency, Ministry of the Interior.*
   C. Because of the growth of the digital environment, government has to concern computer forensic issues seriously. It is a good start right now.
   D. Yes, government indeed thinks that the computer forensics is an important issue. The national standards and national SOPs should be created as soon as possible.
   E. To my best knowledge, MJIB considers computer forensics issues seriously, and already built a *Cyber Forensics Laboratory*. In this situation, the *Cyber Forensics Laboratory* can provide creditable digital evidence for a court. Thus, the official standpoint towards computer forensics is that it can help to investigate high technical crimes.
   F. Due to the activities for a court, computer forensics should be concerned carefully.
   G. No, government does not care about the issues of computer forensics.
   H. Yes, it is a good start right now.
   I. Government is starting to concern computer forensics issues. After the understanding of computer foreniscs, it is discovered that computer forensics indeed helps for crime investigatoins, and governement is starting to develop

relavant projects and to organize the funds for further research and advanced applications.

J. Government is starting to concern computer forensics issues. It is the beginning stage for government to concern the issues.

2. What is your opinion on the current developments within computer forensics? Are you satisfied with the current developments of computer forensics? Why?

A. Performing computer forensics needs outstanding investigators and latest equipments. However, the budgets, investments, and education programs from government are limited. Therefore, it can be considered that the developments and applications of the computer forensics are obstructed by the above reason.

B. Performing computer forensics needs investigators with special skills and particular equipments. Form my point of view, it is the starting stage to consider the computer forensic issues in Taiwan. The current situation in Taiwan is that MJIB, and *CIB, National Police Agency, Ministry of the Interior* both have the ability to deal with computer forensic issues. However, they cannot deal with astronomical cases since the shortage of computer forensic manpower.

C. SOPs and the developments of relevant tools are lacking in the field of computer forensics

D. The development of computer forensics is an ongoing project. We should put more emphasis on building SOPs and trainging computer forenisc investigators.

E. The satisfactory level is 50 out of 100. Unlike forensic science or other computer issues, only the particular group recognizes the importance of computer forensics. At this moment, there is no SOPs. Moreover, from the technical perspectives, more investments should be made for the relevant developments.

F. The current situation of computer forensics in Taiwan is that MJIB, and *CIB, National Police Agency, Ministry of the Interior* have particular departments to deal digital crimes. It is hoped that the manpower and the equipments of computer forensics are going to be recruited and expanded.

G. America and Israel have studied the computer forensic techniques for a long time. However, the current situations of computer forensics in Taiwan are that we do not put too much emphasis on this field, and basically use relevant foreign tools.

H. From my point of view, I am marginal satisfied with the current situation of computer forensics in Taiwan. This is because the developments of the technique are continuing. On the contrary, people with the background of law do not completely understand computer forensics.
I. No opinion.
J. The current development of computer forensics is just a beginning. Government should put more emphasis on recruiting manpower and funding relevant activities.

3. How many years has computer forensics existed as a discipline in your country?

A. MJIB, and CIB have particular departments for computer forensic purpose, and this issue has been concerned for 4-5 years.
B. Around 4-5 years
C. This is not my specialty
D. Around 4-5 years
E. Police force recognizes the computer forensic issues long time ago. The first academic research is around year of 2000. In addtion, MJIB set up the first laboratory for computer forensic purposes in Taiwan.
F. I cannot find evident data to answer this question.
G. Around 7-8 years.
H. Around 5 years.
I. Since the first official laboratory, *Cyber Forensics Laboratory*, was built on Dec 26th 2006, I think the answer of this question is 'less than one year'.
J. Common consensus is built since two years ago.

4. Is computer forensics a topical issue in your country?

A. From my point of view, I think that most of people know that the importance of computer forensics, but unfortunately it is not a topical issue.
B. Compouter forensics is not a very topical issue.
C. Compouter forensics is not a very topical issue.
D. Compouter forensics is not a very topical issue.
E. From the academia point of view, I think it is a topical issue.
F. Yes, there are many discussions in the academic research.

G. Computer forensics receive average attentions within the field of computer security.
H. Compouter forensics is not a very topical issue.
I. Computer forensics is a quite new and young issue. I would not say it is a topical issue, since the fruitages of computer forensics are not realized by government agencies and public.
J. Compouter forensics is not a very topical issue.

Section 2: Procedures of Computer Forensics

5. From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?

A. The SOPs contains: Preparation, Documentation, Collection, Authentication, Analysis, Preservation, Production, and Reporting.
B. I declared the importance of SOPs in 2003. However, there is no SOPs at this moment.
C. This is not my specialty.
D. Generally speaking, SOPs proposed by professor I-Ling Lin and procedures adapted from American standards are used.
E. At this moment, we have official SOPs which is based on the general evidence collecting principles for police force. There are several government agencies and research units trying to create computer forensic SOPs for a particular purpose. To my best knowledge, MJIB is building SOPs at this moment.
F. This is not my specialty.
G. *CIB, National Police Agency, Ministry of the Interior* has Investigating Crime Principles for Police Force as norms for police investigations. In Chapter 6 Section 14, some criteria for computer crime preparation, computer crime searching, and computer crime evidence analysis are listed. As far as I know, MJIB has similar SOPs.
H. Collecting digital evidence, analysing digital evidence, preparing for the report, and presenting in a court.
I. Currently, there is no SOPs. The most important thing for developing a SOPs is that the contents of a SOPs must match the legislation. Thus, MJIB is using other foreign SOPs as norm to modify in order to produce a suitable SOPs.

J. Currently, there is no SOPs. SOPs need to be set up depend on the needs of different agencies.

6. What is your opinion on the importance of SOPs of computer forensic investigations?

A. Personally I think, the most important factor of digital evidence is its validity in a court, and this is very hard to be confirmed without a SOPs.

B. I think a SOPs is very important. A computer forensic SOPs is the key point of the validity of digital evidence.
C. The integrity and accuracy of the results of a computer forensic investigation are able to be confirmed with a SOPs.
D. Having a SOPs is very important, since it is meaningful and fundamental in the field of computer forensics.
E. In order to have better performance, and in order not to make any tiny mistake, a SOPs is necessary. In addition, a SOPs not only can ensure the validity of the digital evidence, but also can make sure any further test from other agencies will produce the same results.
F. A computer forensic SOPs is a standard for a judge, a lawyer, a plaintiff, or a defendant to examine the validity of digital evidence.
G. A computer forensic SOPs is significant for the validity of digital evidence.
H. A computer forensic SOPs is the fundation of the authenticity of the digital evidence.
I. I think a computer fornsic SOPs is necessary for the integrity, and non-repudiatoin of digital evidence. Due to the development and execution of a computer forensic SOPs, the validity of digital evidence is provable and verifiable.
J. Having a SOPs is very important.

7. Based on your knowledge, is there any regulation about the time period to keep digital evidence after the trial? If "YES", how long is the time period?

A. There is no clear regulation for the preserving time of digital evidence after a court session. Personally I think every computer forensic report, and relevant

digital evidence should preserve at least three years. In addition, the digital information for criminal cases should be preserved forever.

B. There is no explicit regulation for the preserving time of digital evidence after a court session.
C. This is not my specialty.
D. I do not clearly understand this issue.
E. To my best knowledge, there is no regulation for the preserving time of digital evidence after a court session. It follows the preserving rules of general (physical) evidence.
F. No, there is no regulation about this issue.
G. I do not clearly understand this issue.
H. There is no explicit regulation for the preserving time of digital evidence after a court session.
I. After I visited the relevant computer forensic laboratories in America, I found that the digital evidence will be preserved after a court session at least 5 years. However, there is no such regulation in Taiwan.
J. There is no explicit regulation for the preserving time of digital evidence after a court session.

Section 3: Characteristics of Computer Forensics

8. Based on your knowledge, what are the main characteristics of digital evidence? (e.g. ***Integrity***)

A. Digital evidence is easy to be damaged and is able to be duplicated completely. For example, digital evidence may be changed due to improper process. Moreover, the original data is not understandable and the number of data may be enormous.
B. Not understandable, easy to be damaged, hard to identify original user, able to be duplicate, and contain meta-data.
C. Consistency, and integrity.
D. Consistency, easy to be damaged, integrity, and admissibility.
E. Easy to be damaged, hard to retrieve, original data is not understandable, and Admissibility
F. I think the consistency issue is deeply interrelated with admissibility. In addition, the major characteristic of digital evidence is that it is very hard to

identify original user.

G. Can be duplicated, hard to eliminate, hard to identify original user, and integrity.
H. Easy to be damaged, and can be duplicated.
I. Easy to be damaged, easy to be duplicated, consistency, and diversity.
J. Non-repudiation.

9. What is your opinion on meta-data of digital evidence from computer forensic perspective?

A. Computer forensic investigators must notice the following three principles: 1. collecting digital evidence without damaging or changing the evidence, 2. proving the examined digital evidence is exact the same as the collected one, and 3. analysing the digital evidence without changing or modifying the original evidence.
B. Meta-data is a unique characteristic of digital evidence. On the contrary, physical evidence cannot provide such data.
C. Meta-data may be produced while the process of computer forensics is proceeding.
D. Meta-data is the data for digital evidence, and is also the key point of the success of a computer forensic investigation。
E. No opinion
F. This is not my specialty.
G. Credible software is needed to be meta-data.
H. I do not understand this question.
I. Meta-data is very useful information for computer forensics. This is because normal users do not understand the format of meta-data, and this makes them hard to modify the meta-data. Thus, meta-data itself can be considered another type of digital evidence.
J. Meta-data can become a vigorous reference.

10. What is your opinion on the trustworthiness of meta-data of digital evidence?

A. Meta-data comes from different sources affects its quality and trustworthiness.
B. I think the trustworthiness of meta-data is not a problem, as long as the meta-data is examined by qualified computer forensic tools.

C. The trustworthiness of meta-data is affected by the quality of the computer forensic tools.
D. The trustworthiness of meta-data should be acceptable, unless it is changed by computer experts, such as hackers.
E. No opinion.
F. This is not my specialty.
G. The trustworthiness of meta-data is variable. For example, if computer forensic investigators are able to prove the validity of procedures and the integrity of the digital evidence, the meta-data is trustworthy. Otherwise, it is not trustworthy.
H. I do not understand this question.
I. From my understanding, I think the format of meta-data is based on the design of the original inventor. Thus, unless users are familiar with the format of the file, it is very difficult to change the meta-data. This means that the trustworthiness of meta-data is relatively high.
J. I think the trustworthiness of meta-data is marginal.

11. How would you describe the relationship between computer security and computer forensics?

A. Computer forensics not only helps to discover victimized data, but also is helpful to prevent computer security issues from occurring.
B. The purpose of computer security is to prevent any security issues, and the intention of computer forensics is to discover victimized data. There is no clear and direct connection between computer security and computer forensics. However, I think computer forensics is helpful to strengthen the capability of computer security.
C. The power of computer security can be improved by performing computer forensics.
D. The ultimate goal of computer security is to protect the confidential data from other irrelevant users. Computer forensics focuses on discovering victimized data.
E. Computer forensics is normally considered the investigation after the digital incidents. Besides its original purpose, I think it is helpful to improve computer security. Thus, I think computer forensics should be contained by computer security.

F. This is not my specialty.
G. The relation between computer security and computer forensics is interrelated. For example, computer forensic investigators are needed after computer security incidents. Some system backdoors may be discovered by computer forensic testing.
H. From my interpretation, there are two types of computer forensics. One is for discovering digital problems, and the other is for the court purposes. They both occurred after computer security incidents.
I. If computer security is performed authentically, useful digital evidence, such as security log, can be preserved for further investigations. Thus, the relation between computer security and computer forensics is interrelated, and they can help each other. Having thorough computer security policy is a great help for computer forensics.
J. Computer forensics is the power to animate computer security.

12. When performing a computer forensic investigation, is it necessary to understand the background of the investigated person? (How many dogs they have? What cars they drive? Do they have any habit?) or just focus on analysing the digital data? Why?

A. The motivation of a crime and personal behaviours are affected by personal background. Thus, I think the computer forensic investigators need to realize the background of the suspect rather than merely analysing digital data.
B. Yes, I think it is necessary for computer forensic investigators to understand the background of the suspect, since computer forensic investigators may have the chance to obtain extra information. For example, the password may based on the suspect's birthday.
C. Understanding the backgrounds of investigated person can help to clarify the direction of a computer forensic investigation.
D. I think to understand the background of investigated person is necessary because some left traces or clues may be found. After surveying the backgrounds of investigated person, the computer forensic investigators still need to focus on the issues of digital evidence.
E. There are two different perspectives. One perspective is that computer forensic investigators should only pay attentions on analysing digital evidence, and

interpreting the analysed information. The other perspective is that computer forensic investigators should use any possible information including backgrounds of investigated person to re-assemble the digital incident. Personally I think the later perspective is more helpful for reconstruct the digital incident.

F. Of course, it is necessary to understand the backgrounds of computer forensic investigators. In this manner, the credibility, validity, and reliability of the corresponding computer forensic report are increasing.
G. It is necessary to understand the backgrounds of investigated person since this is a very important part of a criminal investigation.
H. I have no opinion on this question.
I. I think to understand the background of investigated person is helpful for analysing digital data. In this case, it is more likely to abstract meaningful digital information which is truly related to the case. For example, key words are sometimes useful for connecting the digital data with the case.
J. I do not think it is necessary to realize the backgrounds of investigated person. If computer forensic investigators can obtain the relevant information, it is sometimes helpful. However, if computer forensic investigators cannot have the information, the results (digital evidence) are not going to be changed.

Section 4: Organization of Computer Forensics

13. In your country, is the status of a computer forensic organization in law enforcement higher than general police duties? or equal to them? or lower?

A. As far as I know, there are two computer forensic organizations in Taiwan. One belongs *to CIB, National Police Agency, Ministry of the Interior*, and the other is under jurisdiction of MJIB. Thus, the status of computer forensic organizations is higher than general police stations.
B. Higher than general police stations.
C. Higher than general police stations.
D. Higher than general police stations.
E. I think the status of computer forensic organization should equal to general police stations.
F. The particular computer forensic organizations belong to *CIB, National Police Agency, Ministry of the Interior,* and MJIB.

G. Computer forensic organization is one of internal organizations of a police station. Thus, my answer of this question is that status of computer forensic organization is lower than general police stations.
H. MJIB has a cyber forensic labortary which is able to deal with digital incidents and digital evidence.
I. Using MJIB as an example, the status of cyber forensic labortary is higher than general police stations. However, I do not understand the police system.
J. Lower than general police stations.

14. In your country, do law enforcement organizations out-source computer forensic problems?

A. Since there is no famous private company providing relevant services, computer forensic tasks are performed by law enforcement organizations at this moment.
B. At this moment, law enforcement organizations do not out-source computer forensic problems.
C. At this moment, law enforcement organizations do not out-source computer forensic problems.
D. I have never heard about this information.
E. At this moment, law enforcement organizations do not out-source computer forensic problems. However, as far as I know, they are planning to do so.
F. I cannot find evident data for this topic.
G. At this moment, law enforcement organizations do not out-source computer forensic problems. They deal with computer forensic problems by themselves.
H. MJIB has the ability to deal the computer forensic issues. However, MJIB will work with other companies under special situations.
I. To my best knowledge, besides official computer forensic investigators who belong to government agencies, private computer forensic workers are also recruited for the computer forensic tasks in America. In Taiwan, law enforcement organizations do not out-source computer forensic problems at this moment.
J. At this moment, law enforcement organizations do not out-source computer forensic problems.

15. Does the organization/department/agency you work for have policies for computer forensic readiness? If “YES”, can you provide the name of your organization/department/agency? could you please briefly explain the policies.

A. I work for the university. Therefore, it is not urgent for the university to prepare for the computer forensic readiness.
B. I work for the university. At this moment, the university does not have preparations for the computer forensic readiness. However, the university that I work for is preparing to build a computer forensic responding centre.
C. No, the organization that I work for does not have any preparatoin for the computer forensic readiness.
D. At this moment, the organization that I work for does not have any preparatoin for the computer forensic readiness since there is no urgent need.
E. Yes, I work for Taiwan Information Security Centre at Nayional Cheng Kung University (TISCNCKU), and TISCNCKU has preparations for computer forensic readiness.
F. No, the organization that I work for does not have any preparatoin for the computer forensic readiness.
G. No, the organization that I work for does not have any preparatoin for the computer forensic readiness.
H. Yes, I work for MJIB, and MJIB built cyber forensic laboratory on December 2006.
I. The computer forensic issues are dealt in MJIB in reality. Thus, my answer of this question is ‘Yes’.
J. Yes, I work for MJIB, and the policies of MJIB support the developments of computer forensics.

16. In your country, are computer security issues and computer forensics issues dealt by different organization/department/agency? If “YES”, how would you describe the relationship between computer security organization/department/agency and computer forensic organization/department/agency?

A. Computer security issues and computer forensic issues are managed by different organizations. To my best understanding, the cooperation is existed between the organizations.

B. Yes, Computer security issues and computer forensic issues are managed by different organizations. The relationship between these organizations is coefficient. Due to the uniqueness of computer forensics, not every organization understand its importance and characteristics.
C. Yes, Computer security issues and computer forensic issues are managed by different organizations.
D. Yes, Computer security issues and computer forensic issues are managed by different organizations because they are essentially two different issues.
E. Computer security issues are managed by cross-agencies unit. This means that computer security issues are controlled by higher level unit. On the other hand, computer forensic issues are managed by police agencies and/or investigation agencies.
F. From my understanding, *CIB, National Police Agency, Ministry of the Interior* in charges of computer security issues and computer forensic issues at the same time. Therefore, my answer of this question is 'NO'.
G. There is no evident difference between these two agencies.
H. Yes, Computer security issues and computer forensic issues are managed by different organizations. Computer forensic organizations have the ability to prevent digital incidents from occurring, but computer security organizations do not have such ability.
I. Yes, Computer security issues and computer forensic issues are managed by different organizations. In MJIB, there are two different departments to manage computer security issues and computer forensic issues separately.
J. Yes, Computer security issues and computer forensic issues are managed by different organizations. Computer security agencies focus on preventing digital incidents from occurring, and computer forensic agencies focus on retrieving digital evidence.

Section 5: Certification of Computer Forensics

17. How are computer forensic experts produced in your country? through what kind of tests? or procedures?

A. From the perspective of computer forensics, many things need to be learned and improved at this moment. Government does not hold any exam for certifying computer forensic investigators.

B. Normally computer forensic experts are trained by professional courses or by real experience. There is no unified standard to follow at present. For example, Association of Computer Investigative Specialists (IACIS) and TWCERT/CC are two organizations which provide relevant services.
C. This is not my specialty.
D. Computer forensic experts are produced via professional training. For example, these training may provide by central police university. However, I personally do not know the details of the training.
E. The main trend is to obtain foreign certifications, such as American and/or British certifications.
F. I cannot find evident data for this topic.
G. To my understanding, TWCERT/CC does provide the corresponding certifications. The students need to finish the courses, assignments, and exams.
H. Computer forensic experts are produced by professional courses, certifications or real working experience.
I. In MJIB, the computer forensic experts are chosen from investigators with computer backgrounds, and then trained via relevant courses.
J. Computer forensic experts are produced by professional training and real working experience.

18. Do you allow computer forensic experts from other countries to work in a similar job in your country?

A. I think it should have foreign computer forensic experts been invited for the communication purpose. However, I do think that official workers are accepted.
B. If computer forensic experts from other countries are willing to work in Taiwan, it is acceptable. However, this situation does not occur at present.
C. My answer of this question is that it is acceptable for computer forensic experts from other countries to work in a similar job in Taiwan.
D. My answer of this question is that it is acceptable for computer forensic experts from other countries to work in a similar job in Taiwan. For example, Chang-Yu Lee who works as Chief Emeritus for Scientific Services in Connecticut USA. Moreover, the digital evidence may be sent overseas (e.g. USA) for testing.
E. I think the answer is that this situation is acceptable, but there is no example in reality at this moment.

F. I think the expertise of computer forensic investigators should not limit by the nationality.
G. My answer of this question is that it is acceptable for computer forensic experts from other countries to work in a similar job in Taiwan.
H. There is no such situation at this moment.
I. Currently there is no corresponding regulation for this situation. Thus, foreign computer forensic experts are not acceptable to work in Taiwan.
J. Foreign computer forensic experts are not acceptable to work in Taiwan.

19. Does your country have any organization/department/agency for certifying computer forensic experts? If "YES", what are the names of the organizations/departments/agencies? What criteria do they follow?

A. No, ther is no such organization in Taiwan to certify computer forensic experts.
B. No, ther is no such organization in Taiwan to certify computer forensic experts.
C. This is not my specialty.
D. To my understanding, ther is no such organization in Taiwan. However, I think Computer Skills Foundation may provide relevant services.
E. No, ther is no such organization in Taiwan to certify computer forensic experts.
F. I cannot find evident data for this topic.
G. To my understanding, TWCERT/CC does provide the corresponding certifications. The students need to finish the courses, assignments, and exams. The standards are made by TWCERT/CC itself.
H. No, ther is no such organization in Taiwan to certify computer forensic experts.
I. No, ther is no such organization in Taiwan to certify computer forensic experts.
J. No, ther is no such organization in Taiwan to certify computer forensic experts.

Section 6: Training of Computer Forensics Experts

20. Is there any government organization/department/agency willing to support the education/training of computer forensic manpower? or to support the research of computer forensics? Can you briefly explain how the government organization/department/agency supports these agencies?

A. Recently, there are many academic conferences which are held by relevant organizations, such as CPU, Taiwan Academy of Forensic Sciences, CIB,

National Police Agency, Ministry of the Interior, and Institute of Forensic Medicine, Ministry of Justice. The purpose of these conferences is to provide a chance for computer forensic workers to exchange experiences, to have on-the-job training, and to improve the developments of computer forensics.

B. There are many conferences which are held by central police university or MJIB. The purpose of these conferences is to improve the calibre of computer forensic workers.
C. This is not my specialty.
D. Yes, I think government is willing to support the education and/or training of computer forensic manpower. For example, government provides fund for universities, such as CPU, to hold computer forensic conferences. In this manner, computer forensic workers can obtain latest knowledge, learn new skills, and exchange experiences.
E. Form my understanding, police force and MJIB are more or less supportive for the computer forensic research projects, conferences, and workshops。
F. Yes, I think government is willing to support the education and/or training of computer forensic manpower. In addition, academic researchers are trying to build a computer forensic laboratory.
G. Sending computer forensic workers to participate in the courses which are held by companies which produce computer forensic equipments, and/or to attend certification courses is the current situation.
H. Yes, I think government is willing to support the education and/or training of computer forensic manpower. For instance, sending computer forensic workers overseas for the advanced training is an obvious example. Moreover, the budget is given for the research of computer forensic techniques and legal issues.
I. At this moment, government is very supportive for the training and education of computer forensic workers. Thus, the fund is given annually for the training of computer forensic workers.
J. Form my understanding, I think only MJIB has regular training activities.

21. Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this program come from?

A. Holding conferences irregularly is the major way to provide on-the-job training. The teachers mainly come from professors in university, or senior computer forensic investigators in MJIB or *CIB, National Police Agency, Ministry of the Interior*. Furthermore, sending computer forensic workers to foreign organizations for educational courses, such as EnCASE training courses, is another method.
B. From my understanding, conferences are considered on-the-job training. Moreover, computer forensic workers may be trained oversea. This is not a regular project.
C. This is not my specialty.
D. My answer of this question is 'Yes'. However, I only attended for the on-the-job training once. I am not sure about the situation after the training.
E. I do not know the answer of this question.
F. I cannot find evident data for this topic.
G. I do not know the answer of this question.
H. Yes, on-the-job training programs are provided irregularly for computer forensic investigators in Taiwan. Normally people are sent overseas for training.
I. At this moment, most of on-the-job training programs are held irregularly in MJIB. The experts belong to professional companies are invited to be the teachers of these training programs.
J. MJIB is holding on-the-job training programs annually.

22. In your country, do you have methods to train computer forensic experts? If "YES", can you briefly explain?

A. Besides the relevant computer forensic training courses which were held by TWCERT/CC, there is no similar method to train computer forensic investigators in Taiwan. Thus, I think the computer forensic investigators are sent to overseas for advanced training.
B. Yes, there are methods to train computer forensic experts. For example, the service provided by TWCERT/CC. However, this is not the only choice and is not compulsory.
C. This is not my specialty.
D. The answer of this question is 'Yes'. The government agencies commended professor I-Ling Lin who works in CPU to formulate the related plans.

E. I do not know the answer of this question.
F. I cannot find evident data for this topic.
G. From my understanding, there are courses which are held by TWCERT/CC.
H. Computer forensic investigators are sent overseas to be trained.
I. Computer forensic investigators are sent overseas to the foreign computer forensic organizations to be trained, or are trained by relevant computer forensic courses.
J. Computer forensic investigators are trained by foreign tests.

23. Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?

A. I personally think that computer forensics is a job requiring highly technical backgrounds. The ability of computer forensic experts must include operating system, network, software, hardware, computer forensic procedure, and legal issues. Therefore, the training courses must follow high standards. The cultivation of a computer forensic expert can be done by professional certifications.
B. This is a complicated job. I think to train a computer forensic expert at least needs 1~2 years.
C. This is not my specialty.
D. I think a computer forensic investigator should be trained continually since the developments of computer forensics are ongoing. In this case, computer forensic investigators have the ability to face the challenges brought by intruders or hackers.
E. I think it needs 1~2 years to cultivate a computer forensic investigator with basic capabilities.
F. The field of computer forensics contains many different subjects. Thus, I think a computer forensic investigator should be trained continually.
G. I think to train a computer forensic expert needs 2~3 months.
H. I do not know the answer.
I. I personally think to train a computer forensic expert at least needs 1 year. The most suitable time is 3 years.
J. I think to train a computer forensic expert needs 1 year.

Section 7: Skills of Computer Forensic Experts

24. What is your opinion concerning the importance of hash functions in the field of computer forensics?

    A. Hash function is meaningful for preserving digital evidence, and it can eliminate possible changing of digital evidence.
    B. Hash function is very important. This is because it can ensure the relation between original digital evidence and its copy.
    C. This is not my specialty.
    D. Hash function can be used to encrypt the data, or to protect data from being changed or stolen.
    E. Hash function is a very important procedure for testing digital evidence. However, the collision issue of hash functions is rarely be concerned. Perfect hash function is rarely be concerned.
    F. Hash function is useful to solve the consistency and authentication issues of digital evidence.
    G. Hash function can be used to verify the relation between original digital evidence and its copy.
    H. Hash function is helpful for the authentication of digital evidence. My interpretation of authentication is the authentication of the entire process, which contains collecting digital evidence, analysing digital evidence, reporting digital evidence, and presenting digital evidence.
    I. Hash function can be used to prove the integrity and consistency of digital evidence.
    J. Hash function is importatn to ptotect digital evidence from changing.

25. Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?

    A. The collision of hash function shows that it is possible to forge and to change the digital evidence. Therefore, the digital evidence will become questionable.
    B. The collision of hash function makes it more difficult to perform computer forensics. For example, an investigator may need to use several hash functions to check the relationship between original digital evidence and its copy.

C. This is not my specialty.
D. With the collision of hash function, it cannot guarantee the relationship between original digital evidence and its copy.
E. Once the hash function, which is used to check the validity of original digital evidence, has collision issues, the digital evidence may become unacceptable or be overrided. However, I think this situation may only occur in the near future. I think the solution for this situation is to use longer hash bit to prevent the collisions. Moreover, perfect hash function is the answer for this predicament.
F. This is not my specialty. I cannot answer this question.
G. Due to the collision of hash function, the investigator may be confused by the relation between original digital evidence and its copy. However, the possibility for collision is very low. The solution for this situation is to use more than one hash function to check the relationship between original digital evidence and its copy.
H. I do not know the answer of this question.
I. The collisions of hash functions have certain impacts on the integrity and consistency of digital evidence. Thus, the credibility of digital evidence is affected.
J. I think the collision of hash function does not have influences on computer forensics.

26. Based on your knowledge, what are the countermeasures within computer forensics to the collisions of hash functions?

A. The collisions of MD5 and SHA-1 were found. Thus, more secure hash functions, such as SHA-224, SHA-256, SHA-384, and SHA-512 should be use so as to protect the safety of the data.
B. From my understanding, using more than one hash function to check the validity of digital evidence is a well-accepted countermeasure.
C. This is not my specialty.
D. Before processing original digital data, computer forensic investigators need to ensure the quality of the used methods.
E. Perfect hash function.
F. This is not my specialty.

G. Using more than one hash function to check the validity of digital evidence is a well-accepted countermeasure.
H. I do not understanding this question.
I. If the researchers can develop new hash function, this is very useful for maintaining the integrity of digital evidence.
J. Using more than one way to test the result.

Section 8: Bottlenecks within Computer Forensics

27. Based on your knowledge, have computer forensic investigations in your country ever encountered problems which are caused by time-stamps? or by different time zones? If "YES" how you deal this type of problems?

A. Using the time-stamp services, which are provided by Internet Engineering Task Force (IETF) and/or National Institute of Standards and Technology (NIST), to solve the problems caused by different time zones.
B. No, there is no such problem because of two reasons. First of all, there is only one time zone in Taiwan. Second of all, 'time' is an important issue for computer forensics. To figure out the issues caused by 'time' is a basic task for computer forensic investigator.
C. This is not my specialty.
D. Using local time or attack time as the standard to solve the time problems.
E. From my best understanding, this is not a serious issue. The solutions for problems caused by time-stamp and /or different time zones are normally provided by training courses.
F. I have met any similar issue.
G. In order to solve this problem, I would suggest to seek for his Internet section. Comparing this information with local time is a way to solve the problems caused by time-stamp and different time zones.
H. I do not think time-stamp and time zone are problems. In practice, time is an important and fundamental issue for investigating digital crimes. From the computer forensic perspective, it is useful to record crime scene records by time. Moreover, we have to learn a lot of things from foreign experiences.
I. I think time-stamp is not a trouble, since it is rarely used. Moreover, I think time zone is not a problem neither, since there is only one time zone in Taiwan. From my experience, the problems caused by different time zones can be fixed by

computer forensic software.

J. I have met any similar issue.

28. Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country?
(1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%

A. According to my understanding, the percentage of encrypted data within computer forensic investigations is relatively low. Thus, I think 0%-20% is a reasonable answer.
B. 0%-20%
C. This is not my specialty.
D. I do not know since I am not actually involved in a computer forensic investigation.
E. No opinion.
F. I do not have actual data to answer this question.
G. 41%-60%。
H. 0%-20%。
I. According to the encountered cases, I discover that the percentage of encryption data is around 21%-40%.
J. 0%-20%。

29. Based on your knowledge, how do computer forensic investigators deal with the encrypted data in your country?

A. Using relevant tools to decrypt the data.
B. From my understanding, there are two ways to deal with this situation. The first way is to try to decrypt the data, and the second way is to use alternative evidence.
C. This is not my specialty.
D. The investigator normally tries to break the encryption. If this action does not work, the investigator will seek evidence from other possible sources.
E. No opinion.
F. This is not my specialty. I cannot answer this question.
G. Using decryption software.

H. Asking the suspect for the decryption key or using brute force to break the encryption. Unlike USA, we do not use warrant or install keylogger.
I. Using powerful or popular decryption software decrypts the data. Moreover, if the data is encrypted by the private and/or special encryption algorithm, unique methof is needed.
J. Decryption.

30. Based on your knowledge, have performing computer forensic investigations in your country suffered any difficulty? Can you briefly list them?

A. 1. Traditional forensic investigators do not have the ability for computer forensics, 2. law enforcements should have the same level of understanding of computer forensic issues, 3. computer forensic laboratory should have better hardware and software, and 4. international digital crimes are hard to trace.
B. There are at least three problems. The first problem is that the lack of manpower. The second problem is that the training for the existing computer forensic investigators are not enough. The third problem is that the variety of the computer forensic tools is insufficient.
C. 1. The number of technical investigators is insufficient, 2. there is no SOPs, and 3. the use of computer forensic tools.
D. The major difficulty is that the victim does not report the case due to the reputation or commercial benefit.
E. 1. New technology is releasing, and 2. there is no related database for comparasion.
F. The seizure and interpreting of large scale database.
G. 1. There are not enough computer forensic tools, including hardware and software, and 2. it is hard to recovery the critical data sometimes.
H. 1. Investigators without technical backgrounds do not understand computer forensics, 2. computer forensics is a time consuming job, 3. it is hard to define the items which are needed to be seized, and 4. if the items are too many, how to seize becomes a problem.
I. I think the most difficult part of a computer forensic investigation is to retrieve digital evidence from large companies. This is because a large company normally use diverse storage devices and the scale of these digital devices is very large as well.

J. The techniques for performing computer forensics, and the computer forensic equipments are not sufficient. Furthermore, too much data is another serious issue.

31. "*Technical Issues*" and "*Human Issues*" are two separate things. It is easy to examine misuse of a computer, but how to prove the suspect is the one who actually caused this misuse is not an easy task. Based on your knowledge, how do computer forensic investigators deal with this problem in your country?

A. Generally speaking, there are limitations for user authorization within an organization. Thus, this information is helpful for identify computer misuses.
B. This question can be solved by the cooperation with traditional investigation method, such as surveillance cameras.
C. This is not my specialty.
D. This is a very hard problem to solve. I think the best solution is to use video type or to check IP address to trace corresponding criminals.
E. Normally traditional investigation methods are used to overcome this problem. Most computer forensic investigators cooperate with traditional investigators in order to overcome this problem.
F. This is not my specialty, since I am not a computer forenisc investigator. However, from my best understanding, other types of evidence can be used if the authenticity of digital evidence is questioned.
G. Using other evidence as major evidence is an alternative way to solve this problem. For example, criminals need to withdraw money via ATM or actual counter for a Internet fraud. This means relevant traces are left, and these traces can be used to identify the corresponding criminal.
H. This question does not belong to the scope of computer forensic workers. This issue is actually a legal problem. Combining digital evidence and other evidence may helpful for the crime scene reconstruction.
I. There are two means to prove that the suspect is the person who actually used the computer. The first method is to examine other information within the seized computer, such as pictures. The second method is to examine the computer hardware rather than software. For example, testing fingerprints and/or DNA left on the computer hardware. However, I think this problem is beyond the scope of my job.

J. This question is prosecutor's job. I only present what I examined.

Section 9: Interaction in Computer Forensics

32. Based on your knowledge, have computer forensic organizations/departments/agencies in your country ever had interactions with international organizations/departments/agencies related to similar area? If "YES", how do they interact with other organizations/departments/agencies in other countries?

A. I can think of four ways to do the international interactions. 1. Sending computer forensic workers to visit other organizations, 2. Sending computer forensic workers to attend educational courses, 3. Sending computer forensic workers to attend international conferences, and 4. Building relationship with other international interactions.
B. From my best understanding, attending international conferences, and sending computer forensic workers oversea for educational and research purposes are two approach normally used.
C. This is not my specialty.
D. It is normal for investigation organizations to send computer forensic workers oversea to study and/or to perform research. In addition, foreign computer forensic experts are sometimes invited for educational purposes.
E. From my best understanding, the common ways to interact with other international organization are to visit them and/or to invite their experts for a speech. However, I do not know the details of actual cooperations.
F. Exhibiting conference is a common way to interact with other international organizations.
G. 1. Sending computer forensic workers to attend international conferences, and 2. Sending computer forensic workers overseas to visit relevant orgnaizations and/or for education purposes.
H. 1. Sending computer forensic workers to attend international conferences, and 2. Sending computer forensic workers overseas to visit relevant orgnaizations, and vice versa.
I. At present, Cyber forensics Laboratory of MJIB sends computer forensic works regularly (annually) to International Association for Computer Information Systems (IACIS) to be trained. Moreover, Cyber forensics Laboratory also has

connection with other famous computer forensic organizations.

J. 1. Sending computer forensic workers overseas to visit relevant orgnaizations, and 2. The other usual way is to invite computer forensic experts to give speeches.

33. Based on your knowledge, in your country have computer forensic organizations/workers ever had interactions with other computer forensic organizations/workers? If "YES", how do they interact with each other?

A. I can think of four ways to do the national interactions. 1. Inviting computer forensic workers to give a speech or to teach relevant courses, 2. computer forensic researchers can provide professional opinions, 3. computer forensic researchers can work as consultants, and 4. Holding conferences is a good way for national interaction.
B. 1. Attending conferences is a good way for national interaction, and 2. computer forensic researchers can work as consultant.
C. This is not my specialty.
D. The answer is the same as previous question.
E. Generally speaking, the interaction is normally based on doing research project together.
F. Holding conferences is a good way for national interaction.
G. 1. Holding conferences is a good way for national interaction, and 2. Performing research project together is a good way for national interaction.
H. 1. computer forensic workers can work as consultants, and vice versa, and 2. Attending conferences is a good way for national interaction.
I. Attending conference or holding discussion forum is a good way for interaction.
J. Attending discussion forum is a good way for interaction.

34. Based on your knowledge, employees in the field of computer forensics normally interact or share their professional experiences with (1)colleague (2)supervisor (3)others (please explain)

A. Colleague and supervisor.
B. Colleague.
C. Colleague and supervisor.

D. It is a good opportunity to share and to exchange experience with other pepople in the conference.
E. Colleague, other academic researchers or technical workers.
F. I will share my personal experience with the people related to the case.
G. Colleague, supervisor, and relevant people in Internet.
H. Colleague, and other technical people.
I. I will share my personal experience with colleagues. Furthermore, I sometimes exchange experience with experts who belong to other agencies.
J. Colleague.

Section 10: Court Aspects of Computer Forensics

35. In your experience, do courts give a high or low weighting to digital evidence in your country?

A. I think courts give a high weighting to digital evidence.
B. From my understanding, courts give a low weighting to digital evidence. This is because the members of the court do not entirely understand digital evidence.
C. From my understanding, courts give a low weighting to digital evidence.
D. From my understanding, the court realizes the importance of digital evidence. However, because the digital evidence can be modified easily, judge may not trust it.
E. From my understanding, courts give a high weighting to digital evidence. However, digital evidence is rarely used in a court in reality.
F. The weighting of digital evidence depends on the characteristics of the case.
G. From my understanding, courts give a low weighting to digital evidence. Digital evidence is treated as accessory evidence in most situations.
H. From my understanding, courts give a low weighting to digital evidence. This is because the members of the court do not entirely understand digital evidence.
I. From my personal experience, the weighting of digital evidence depends on the characteristics of the case. If it is a computer related crime, the weighting of digital evidence within a court is considered high. On the contrary, if it is a traditional case, the weighting of digital evidence within a court is considered low.
J. I think courts give a high weighting to digital evidence.

36. Do you know of any difficulties caused by using digital evidence in court? If “SO”, what has been the major reason for this?

A. In order for a court to admit the digital evidence, computer forensic investigators must prevent it from modifying, and preserve it safely. Therefore, a proper procedure is needed to collect, and to analyse the digital evidence so as to present digital evidence in a court.
B. The members of the court do not entirely understand digital evidence.
C. The answer of this question is ‘Yes’.
D. From my understanding, the court realizes the importance of digital evidence. However, because the digital evidence can be modified easily, judge may not trust it.
E. The main reason is that the reliability and trustworthiness of digital evidence is doubted by the judge.
F. Members of the court mainly have legal background rather than computer background. Thus, it needs additional time and efforts to convince them that digital evidence is reliable and trustworthy.
G. The number of cases which are associated with digital crime is not enough. Thus, judges and prosecutors do not entirely understand digital evidence.
H. Members of the court do not entirely understand digital evidence.
I. Presenting digital evidence may need additional equipments, due to the diversity and characteristics of digital evidence. At this moment, digital evidence is normally presented in a court staticly rather than dynamicly. If people have to present digital evidnece in a court in a dynamic way, I think this causes trubles. Thus, I do not think presenting digital evidence causes any difficulties in a court at present.
J. I can think of three difficulties. 1. presenting digital evidence is difficult, 2. explaining the digital evidence is difficult, and 3. members of the court do not have basic concepts of digital evidence.

37. Based on your knowledge, is it the suspect’s obligation to provide digital evidence in your country? Does you country have any law to define such an obligation? If “YES”, Can you provide the name of the law?

A. From my understanding, suspect does not have obligation to provide digital evidence.
B. The answer of this question is ‘No’.
C. This is not my specialty.
D. I do not know if there is a law which defines this issue. However, I think the suspect is willing to provide the digital evidence if he or she thinks that he or she is innocent. On the contrary, the suspect is not going to provide the digital evidence if he or she is guilty.
E. I do not think there is such a rule. However, from my understanding, suspect is allowed to provide evidence which is helpful to himself or herself. In here, I am not sure ‘does the evidence include digital evidence?’.
F. Defendants in Taiwan do not have the obligation to provide evidence, including digital evidence. According to criminal law, this is prosecutors’ responsibility.
G. The answer of this question is ‘No’.
H. I think this question is about ‘Who is responsible for providing digital evidence?’ rather than ‘is it the suspect’s obligation to provide digital evidence?’. In Taiwan, civil law and criminal law do not have such rules.
I. In Taiwan, the law does not ask suspect to provide digital evidence. This is not suspect’s obligation. However, from my understanding, suspect can provide evidence, including digital evidence, which is helpful to himself or herself.
J. I do not know the answer of this question.

38. Based on your knowledge, does the development of the computer forensic technology beyond the development of the current law in your country? If “SO”, does this affect the attitude of computer forensic investigators to perform investigations? If “YES”, can you briefly explain?

A. In seems that the current criminal behaviours in Internet are always beyond the current law. Therefore, I think this situation is likely to affect the attitude of computer forensic investigators to perform investigations. Computer forensic investigators may become inactive because they do not have rules to follow.
B. I agree that development of the computer forensic technology beyond the development of the current law. This may cause the destructive for computer forensic investigators.

C. I agree that development of the computer forensic technology beyond the development of the current law. I think this situation makes digital evidence unacceptable.
D. I do not think this situatoin affect the attitude of computer forensic investigators. This is because any type of evidence is valid in a court.
E. I agree that development of the computer forensic technology beyond the development of the current law.
F. I agree that development of the computer forensic technology beyond the development of the current law. Lawyers and prosecutors rarely focus only on digital evidence. The judge rarely expresses his or her opinion about the suitability of digital evidence. From my personal experience, I have never seen the failure of a case caused by digital evidence which is collect inappropriately.
G. I agree that development of the computer forensic technology beyond the development of the current law.
H. I agree that development of the computer forensic technology beyond the development of the current law. In USA, they improved their civil law for the digital evidence collection and procedures on 01/12/2006. However, the civil law in Taiwan does not provide such details. For example, there is no rule for 'who is going to pay for the expenditure of collecting and analysing digital evidence?'.
I. In Taiwan, the development of computer forensics is at the beginning stage. Thus, the relevant law needs to be improved. This situation indeed affects computer forensic investigators.
J. I do not agree that development of the computer forensic technology beyond the development of the current law.

Section 11: Personal Preference of Computer Forensics Experts

39. As a computer forensic professional, do you use data wiping tools in your work for unnecessary data?

A. I do use data wiping tools.
B. I do use data wiping tools.
C. I do not use data wiping tools.

D. I use data wiping tools for particular information, since it is time-consuming to clean all data. Unless the performance of computer becomes slow, I clean all data in the computer.
E. I do use data wiping tools.
F. I do use data wiping tools.
G. I normally do not use data wiping tools.
H. I do not understand the meaning of this question.
I. I do use data wiping tools.
J. I do use data wiping tools.

40. As a computer forensic professional, do you use any type of encryption tools for the data in your work?

A. I use data encryption tools, such as PGP.
B. Yes, I use data encryption tools.
C. No, I do not use data encryption tools.
D. I use data encryption tools to protect important data. However, it should be noticed that encryption still has certain weaknesses.
E. Yes, I use data encryption tools.
F. Yes, I use data encryption tools. I normally use inbuilt encryption functions within software.
G. Yes, I use data encryption tools.
H. I sometimes use data encryption tools.
I. I use data encryption tools in most situations. However, sometimes I choose not to use the data encryption tools, since it is very difficult to remember various passwords.
J. I sometimes use data encryption tools.

Appendix 10: The Results of Second Round Questionnaire for Delphi Survey in Taiwan (Chinese Version)

1. 在台灣，數位鑑識這個議題的發展約在 4~5 年前。至於相關數位鑑識實驗室則是於 2006 年底建立。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 3 題：數位鑑識在貴國成立的年數(時間)有多久?***)

   A. 是。

   B. 贊成。

   C. 否，不清楚。

   D. 贊成。

   E. 贊成。

   F. 贊成。

   G. 是。

   H. 贊成。

   I. 是。

   J. 數位鑑識之議題，應從學術面與實務面來看，就比較清楚其差異性。

2. 在台灣，基於認知的不同或是單位的不同，目前有多套標準可以參考(由 2.1 可以看出)，但是一個明確的數位鑑識 SOPs 並不存在。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 5 題：依您所見，在貴國執行數位鑑識時可以依循的標準程序(Standard Operation Procedure)為何?***)

A. 是。

B. 贊成，從 2003 年本人提倡 SOPs 至今，結至目前為止並沒有一個統一的版本。

C. 是。

D. 贊成，一個全國的 SOPs 本來就不是一件容易的事。

E. 贊成。

F. 贊成。

G. 是。

H. 是。應由各機關自行訂定，但是必須符合法令之要求。

I. 是。

J. 目前是不存在，不是不可能，而是由誰來訂，如何訂定。非常高難度。目前 FBI 及 USSS 等單位亦是自己訂自己的 SOPs。

3. 數位證據的主要特性可以被歸類為 12 項(由以下圖表可知)。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 8 題：據您所知，數位證據的主要特性是什麼? 例如: 一致性(Integrity)***)

A. 是。

B. 贊成。

C. 否，數位證據的主要特性應該有一定的標準，且由具高度公信力的單位提出。

D. 贊成。

E. 贊成。另外加註一下：這 12 特性，就字面上來看其實有所衝突之處，如不易銷毀、易破壞；多樣性、一致性…等。因此如果能在更進一步地

先行分類，如：數位證據取得時的特性、當成呈堂證據時的特性等，可能較能呈現這些被歸納的數位證據特性。

F. 贊成。

G. 是。

H. 不易取得、不易銷毀、不可否定性，未必屬於通常普遍之特性。具有中介資料，並不了解其意義。

I. 是。

J. 無意見(沒作答)。

4. 數位證據中所呈現的中介資料(例如：時戳)，在數位調查中扮演著相當重要的角色。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 9 題：從數位鑑識的觀點來說，您怎麼看待數位證據中所呈現的中介資料(meta-data)?***)

A. 是。

B. 贊成。

C. 是。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。

H. 贊成。

I. 是。

J. 無意見(沒作答)。

5. 只要符合程序並且使用合格的工具，數位證據中所呈現的中介資料的可信度將不是問題。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 10 題：您認為數位證據中所呈現的中介資料的可信度(trustworthiness)為何?***)

A. 否，可信度視情形而定。

B. 贊成。

C. 是，不過「程序」必須經過確認。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。

H. 否。數位資料還是必須依賴環境證據加以佐證，以強化其真實性。

I. 是。

J. 無意見(沒作答)。

6. 一般來說，在台灣，實務單位(例如：法務部調查局)對於數位鑑識是有所準備，然而非實務單位(例如：各大學)對於數位鑑識並沒有相同的準備也沒有相同的需求。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 15 題：您的工作單位對於數位鑑識是否有所準備? 如果有，請您提供貴單位的名稱。同時，請您簡單說明這些政策。***)

A. 是。

B. 贊成。警大有在準備成立相關實驗室，我認為一般的非實務單位應該沒有這樣的需求。

C. 是。但是大學屬於被動的角色，即使有需求，也必須由上級單位強制實施。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。但是不是所有實務單位數位鑑識都有準備。

H. 否。只要有訴訟需求，就有數位鑑識的需求。

I. 是。

J. 是。但是我要強調各學校之需求，主要在系所主管之看法。

7. 在台灣，確實有提供數位鑑識調查員的在職訓練，主要是不定期。師資來源雖然都是數位鑑識領域的專家，但是並不是單一來源。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 21 題：就您所知，貴國有提供數位鑑識調查員的在職訓練嗎? 通常多久舉辦一次? 師資來源為?***)

A. 是。

B. 贊成。

C. 是。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。

H. 是。

I. 是。

J. 無意見(沒作答)。

8. 訓練一個調查員成為數位鑑識調查員所需的時間至少為一年。在此之後，數位鑑識調查員必須持續學習。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎? (***原第一回合第 23 題：根據貴國數位鑑識發展的現況，您認為訓練一個數位鑑識調查員所需的時間是多久?***)

A. 是。

B. 贊成。

C. 是。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。

H. 是。

I. 是。

J. 無意見(沒作答)。

9. 雜湊函數的碰撞對於數位鑑識是有影響的。這些影響可能包括：數位證據之證據力受到質疑、增加數位鑑識的難度。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎?(***原第一回合第 25 題：某些雜湊函數的碰撞已經***

被證實(例如 MD4, MD5, and SHA0)，您認為雜湊函數的碰撞對於數位鑑識有什麼影響?)

A. 是。

B. 贊成。

C. 是。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。

H. 否。如同指紋一樣，還是有相同的可能性。只是可能性過低的話，在法庭上是可被接受的。況且，數位證據不可作為犯罪之唯一證據，仍須輔以其他環境證據。

I. 是。

J. 雜湊函數只是要證明原始檔案未被更動之方法之一。且其碰撞機率極低。其對數位鑑識本身證據力影響不大。

10. 在台灣，數位鑑識調查行動所遭遇到的加密資料其百分比應該是相對偏低(0%-20%)，至多不會超過 40%。您對於這樣的說法是否贊成? 請簡述原因。您尚有其他意見嗎?(***原第一回合第 28 題：就您所知，貴國數位鑑識調查行動所遭遇到的加密資料其百分比為何? (1) 0%-20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%***)

A. 是。

B. 贊成。

C. 是。

D. 贊成。

E. 贊成。

F. 贊成。

G. 否，沒有看過正式統計資料

H. 是。

I. 是。

J. 無意見(沒作答)。

11. 在台灣，法庭雖然無法忽略數位證據的重要性，但是法庭普遍來說對於數位證據的採性度偏低。特例是，如果是電腦犯罪，則有關犯罪的數位證據的重視度以及採性度應該是相當高。您對於這樣的說法是否贊成？請簡述原因。您尚有其他意見嗎？(***原第一回合第 35 題：以您的經驗，法庭對於數位證據的重視度(採性度)是高？是低?***)

A. 是。

B. 贊成。

C. 是。

D. 贊成。

E. 贊成。

F. 贊成。

G. 是。

H. 是。

I. 是。

J. 採信度，應從二方面來看，一是本身鑑識報告內容是否完備，清楚。一是法官，檢察官之電腦素養是否足夠，能否接受報告之論述。故對法官、檢察官之電腦鑑識訓練十分重要。

Appendix 11: The Results of Second Round Questionnaire for Delphi Survey in Taiwan (English Translation)

1. In Taiwan, computer forensics was developed around 4~5 years ago, and the Cyber Forensics Laboratory was established at the end of 2006. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, How many years has computer forensics existed as a discipline in your country?, is Question 3 in Round One questionnaire*.**)

A. Yes, I agree with this statement.
B. Yes, I agree with this statement.
C. No, I am not sure if this statement is correct or not.
D. Yes, I agree with this statement.
E. Yes, I agree with this statement.
F. Yes, I agree with this statement.
G. Yes, I agree with this statement.
H. Yes, I agree with this statement.
I. Yes, I agree with this statement.
J. No, I think this question should be viewed from academic perspective and practical perspective in order to find out the answer.

2. Due to different organizations and/or different understandings, there is more than one guideline for computer forensics (confirmed by 2.1). Unfortunately, there is no specific SOPs for computer forensic purpose at this moment. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, From your viewpoint, what Standard Operation Procedure (SOPs) is used to perform computer forensic investigations in your country?, is Question 5 in Round One questionnaire*.**)

A. Yes, I agree with this statement.
B. Yes, I agree with this statement. I proposed the concept of SOPs within the field of computer forensics. However, there is still no SOPs at present.
C. Yes, I agree with this statement.
D. Yes, I agree with this statement. A national SOPs is never an easy task.

E. Yes, I agree with this statement.

F. Yes, I agree with this statement.

G. Yes, I agree with this statement.

H. Yes, I agree with this statement. In addition, I think each organization should have and define its own SOPs for computer forensics. The SOPs needs to obey the requirements of the corresponding laws.

I. Yes, I agree with this statement.

J. Yes, I agree with this statement. There is no such SOPs at present. However, it is still possible to define such a SOPs. For example, FBI and USSS have their own SOPs.

3. According to the table, the characteristics can be classified into 12 different categories. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what are the main characteristics of digital evidence? (e.g. Integrity), is Question 8 in Round One questionnaire*.)**

A. Yes, I agree with this statement.

B. Yes, I agree with this statement.

C. No, I do not agree with this statement. I think there should have some standards for the characteristics of digital evidence, and these standards should be proposed by qualified organizations.

D. Yes, I agree with this statement.

E. Yes, I agree with this statement. In addition, I think these 12 categories should be further classified. For example, the characteristics when people collect digital evidence, the characteristics when people present digital evidence. In this case, it is clearer to describe the concept of characteristics of digital evidence.

F. Yes, I agree with this statement.

G. Yes, I agree with this statement.

H. Hard to retrieve, hard to eliminate, and non-repudiation are not necessary common characteristics of digital evidence. I do not understand the meaning of '*contain meta-data*'.

I. Yes, I agree with this statement.

J. No opinion.

4. The meta-data (e.g. time stamp) of digital evidence plays an important role in a computer forensic investigation. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, What is your opinion on meta-data of digital evidence from computer forensic perspective?, is Question 9 in Round One questionnaire*.)**

   A. Yes, I agree with this statement.
   B. Yes, I agree with this statement.
   C. Yes, I agree with this statement.
   D. Yes, I agree with this statement.
   E. Yes, I agree with this statement.
   F. Yes, I agree with this statement.
   G. Yes, I agree with this statement.
   H. Yes, I agree with this statement.
   I. Yes, I agree with this statement.
   J. No opinion.

5. As long as the procedures and computer forensic tools are correct, the reliability of meta-data of digital evidence is not a problem. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, What is your opinion on the trustworthiness of meta-data of digital evidence?, is Question 10 in Round One questionnaire*.)**

   A. No, I think the trustworthiness of meta-data depends on the different situations.
   B. Yes, I agree with this statement.
   C. Yes, I agree with this statement, but additional attention should be put on procedures of computer forensics.
   D. Yes, I agree with this statement.
   E. Yes, I agree with this statement.
   F. Yes, I agree with this statement.
   G. Yes, I agree with this statement.
   H. No, I disagree with this statement. I think traditional evidence is needed in order to improve the trustworthiness of digital evidence.
   I. Yes, I agree with this statement.

J. No opinion.

6. Generally speaking, in Taiwan, practical organizations (e.g. MJIB) have facilities, processes, and ability for computer forensic issues, but non- practical organizations (e.g. university) do not have equivalent preparations and needs. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Does the organization/department/agency you work for have policies for computer forensic readiness? If "YES", can you provide the name of your organization/department/agency? could you please briefly explain the policies., is Question 15 in Round One questionnaire***.)

A. Yes, I agree with this statement.
B. Yes, I agree with this statement. CPU is preparing to establish a laboratory for computer forensic purposes. In addition, I think normal non-practical organizations may not have such needs.
C. Yes, I agree with this statement. However, I think that managed organizations of universities decide this issue for universities.
D. Yes, I agree with this statement.
E. Yes, I agree with this statement.
F. Yes, I agree with this statement.
G. Yes, I agree with this statement. In addition, I would like to claim that not every practical organization needs to organize computer forensic readiness.
H. No, I disagree with this statement. As long as the lawsuit exists, there are needs for computer forensics.
I. Yes, I agree with this statement.
J. Yes, I agree with this statement. However, I think that the situations in universities are mainly decided by the head of the school.

7. In Taiwan, there indeed is on-the-job training for computer forensic investigators, and these training are mainly held without a fixed schedule. The teachers come from different sources although they are all computer forensic experts. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, do you have on-the-job training program for computer forensic investigators in your country? How often are the programs held? Where does the teacher of this program come from?, is Question 21 in Round One questionnaire*.)**

   A. Yes, I agree with this statement.
   B. Yes, I agree with this statement.
   C. Yes, I agree with this statement.
   D. Yes, I agree with this statement.
   E. Yes, I agree with this statement.
   F. Yes, I agree with this statement.
   G. Yes, I agree with this statement.
   H. Yes, I agree with this statement.
   I. Yes, I agree with this statement.
   J. No opinion.

8. Training an investigator to become a computer forensic investigator at least needs one year. After that, a computer forensic investigator needs to update and to learn all the time. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on the current development of computer forensics in your country, can you estimate how long it takes to train a computer forensic investigator?, is Question 23 in Round One questionnaire*.)**

   A. Yes, I agree with this statement.
   B. Yes, I agree with this statement.
   C. Yes, I agree with this statement.
   D. Yes, I agree with this statement.
   E. Yes, I agree with this statement.
   F. Yes, I agree with this statement.
   G. Yes, I agree with this statement.

H. Yes, I agree with this statement.

I. Yes, I agree with this statement.

J. No opinion.

9. The collision of hash function has influences on computer forensics. These influences may include: reliability of digital evidence, and more difficult to perform a computer forensic investigation. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Collisions were found in several hash functions (e.g. MD4, MD5, and SHA0). What do you think about the impact(s) on computer forensics caused by collisions of hash functions?, is Question 25 in Round One questionnaire***.)

A. Yes, I agree with this statement.

B. Yes, I agree with this statement.

C. Yes, I agree with this statement.

D. Yes, I agree with this statement.

E. Yes, I agree with this statement.

F. Yes, I agree with this statement.

G. Yes, I agree with this statement.

H. No, I do not agree with this statement. Like fingerprint, it is still possible to find the same fingerprints. However, as long as the possibility is real low, the evidence can still be accepted by the court. Moreover, digital evidence is not the only evidence used in a court. Traditional evidence is used in a court as well. Thus, I do not think the collisions of hash functions are problems.

I. Yes, I agree with this statement.

J. Since the possibility of collisions of hash functions is very low, I do not think the collisions of hash functions have impacts on computer forensics.

10. In Taiwan, a computer forensic investigation reasonable encounters 0%-20% encrypted data. In the worst situation, a computer forensic investigation encounters at most 40% encrypted data. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, Based on your knowledge, what kind of percentage of encrypted data situations does a computer forensic investigation reasonable encounter in your country? (1) 0%-***

***20% (2) 21%-40% (3) 41%-60% (4) 61%-80% (5) 81%-100%, is Question 28 in Round One questionnaire*.)**

A. Yes, I agree with this statement.
B. Yes, I agree with this statement.
C. Yes, I agree with this statement.
D. Yes, I agree with this statement.
E. Yes, I agree with this statement.
F. Yes, I agree with this statement.
G. No, I do not agree with this statement since I have seen the official statistic data.
H. Yes, I agree with this statement.
I. Yes, I agree with this statement.
J. No opinion.

11. In Taiwan, although the court cannot overlook the importance of digital evidence, the court normally give a low weighting to digital evidence. The only exception is that the digital evidence is valuable in digital crimes. Do you agree with this statement? Please briefly describe the reasons. Do you have other opinions? (***The original question, In your experience, do courts give a high or low weighting to digital evidence in your country?, is Question 35 in Round One questionnaire*.)**

A. Yes, I agree with this statement.
B. Yes, I agree with this statement.
C. Yes, I agree with this statement.
D. Yes, I agree with this statement.
E. Yes, I agree with this statement.
F. Yes, I agree with this statement.
G. Yes, I agree with this statement.
H. Yes, I agree with this statement.
I. Yes, I agree with this statement.
J. The weighting to digital evidence should be considered from two perspectives. The first perspective is that the completeness of the computer forensic report, and the second perspective is that can the members of the

court accept the report. Thu, computer forensic training is very important to the members of the court.

Appendix 12: Case Study Questionnaire in Australia (English Version)

Current Situation Dimension

1. In your organization, do you have Standard Operating Procedures (SOPs) for the identification, collection, or analysis of digital evidence? If so, were these developed in-house? Please discuss influencing sources.
2. Generally speaking, there are two common means of receiving digital evidence; where evidence is collected by a computer forensic specialist, or where the seizure is conducted by normal non-technical individuals and forwarded for analysis. What are the impacts caused by these two different situations? Is there a difference in the acceptability in court?
3. Do you feel that your department has enough manpower to effectively deal with the computer forensic needs of your jurisdictional scope?
4. In your organization, where do you source new recruits? For example, primarily internally, from law enforcement backgrounds, or based on technical skill?

Policy and Organization Dimension

5. Do you feel that government policy is current with misuse of technology? This may encompass how legislation affects your work, and the bearing and weight that digital evidence is given by courts.
6. In your country, what organizations are consultable to deal with technical issues in digital evidence? This may include government departments and private companies.

Education Dimension

7. Were there any technical prerequisites or qualifications required before you started working with digital evidence? Does your organisation provide any on-the-job training? How long have you been working as a computer forensic investigator?
8. What are the current prerequisites and qualifications for new staff? Are there specific training methods for new employees working with digital evidence in your organisation? Have the forms of training changed since you undertook them?
9. In your country, are there any tertiary-level courses that teach computer forensics?

Law Dimension

10. A) Do you agree with and what is your opinion of the following statement: '*It is necessary for a computer forensic investigator to understand law relevant issues*'?

    B) In your own experience, what is the level of legal knowledge that forensic analysts have?

11. A) Do you agree with and what is your opinion of the following statement: '*It is necessary for members of the court (e.g. lawyers and judges) to understand the technical issues associated with computer forensics*'?

    B) In your own experience, what is the level of legal knowledge that members of the court have?

Personal Preferences and Skills Dimension

12. As a computer forensic professional, do you use data wiping tools and/or encryption tools for your data?
13. How does your organization upgrade the technical skills of its computer forensic specialists? To what extent do you develop in-house courses, attend industry short courses, or sponsor tertiary education?

Appendix 13: Case Study Questionnaire in Taiwan (Chinese Version)

現況層面

1. 國內相關執法機關是否有數位鑑識標準程序(standard operating procedure)? 您工作的單位有 SOPs 嗎? 若有，其來源為何? (效法他國、自行研發…)
2. 一般來說，您都是一開始就參與辦案(例如：親自去現場扣押電腦)；還是由普通員警扣押電腦，再轉交給您執行進一步的數位鑑識工作。兩者對您執行鑑識工作有什麼影響?
3. 貴單位的人力是否足以應付國內數位鑑識的需求?
4. 貴單位中，數位鑑識專家的來源為何? (由資訊室轉調、從新招募…等)

政策與組織層面

5. 數位鑑識相關政策 是否會影響到數位鑑識的執行? 或是影響到您辦案的態度? (例如：法令(不)周全則辦案(不)順利)
6. 國內有那幾個單位有資格、有能力進行數位鑑識? 有任何私人(民營)企業有能力進行數位鑑識嗎?

教育層面

7. 您到職前有通過任何測驗、考試嗎? 有在職訓練嗎? 如何進行? 您大約在何時接手數位鑑識調查員這份工作?
8. 承上一題，目前貴單位對於未來招募的數位鑑識調查員是否有明確的訓練方式? 此方式跟您當初的方式是否相同?
9. 貴國是否有大學院校擁有數位鑑識相關課程?

法律層面

10. 您認為數位鑑識調查員有沒有必要去了解法律相關議題? 實務上，您是否了解國內現行數位鑑識(computer forensics)相關法律?
11. 反之，您認為法律人有沒有必要去了解數位鑑識相關議題? 以您的經驗來說，實務上，國內法律人(例如：法官、律師) 是否熟析您的業務範圍?

人員偏好與技術層面

12. 身為數位鑑識專家，您本身是否有使用加密工具 and/or 清除工具?
13. 隨著數位鑑識工具的推陳出新，相關技術亦必須隨之提升。您在技術方面的更新是透過何種管道? (例如：考證照…)