UNIVERSITY OF DERBY

The Comprehensive Digital Forensic Investigation Process Model (CDFIPM) for Digital Forensic Practice

Reza Montasari

Doctor of Philosophy 2016

Thesis

Submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy (PhD) in Digital Forensics

Director of Study: Dr. Victoria Carpenter
Supervisor: Prof. Richard Hill

June 2016

Table of Contents

LIST OF PUBLICATIONS ..... **III**

LIST OF FIGURES ..... **V**

LIST OF TABLES ..... **VII**

LIST OF ABBREVIATIONS ..... **VIII**

DECLARATION ..... **IX**

ABSTRACT ..... **X**

ACKNOWLEDGMENTS ..... **XII**

CHAPTER 1: INTRODUCTION **1**

1.1 BACKGROUND 1
1.2 RESEARCH PROBLEM 6
1.3 RESEARCH HYPOTHESIS 6
1.4 RESEARCH AIM, OBJECTIVES AND QUESTIONS 7
1.5 SCOPE, LIMITATIONS AND ASSUMPTIONS 9
1.6 RESEARCH CONTRIBUTION 12
1.7 METHODOLOGY 12
1.8 OUTLINE OF THE THESIS 25
1.9 SUMMARY OF THE CHAPTER 26

CHAPTER 2: LITERATURE REVIEW **27**

2.1 INTRODUCTION 27
2.2 DIGITAL FORENSIC INVESTIGATION 27
2.3 DIGITAL EVIDENCE 30
2.4 STANDARDS AND GUIDELINES 40
2.5 METHOD OF IDENTIFYING THE PREVIOUS MODELS 44
2.6 ASSESSMENT CRITERIA FOR THE PREVIOUS MODELS 45
2.7 REVIEW AND ASSESSMENT OF THE PREVIOUS MODELS 49
2.8 ANALYSIS OF MODEL REVIEW AND ASSESSMENT 105
2.9 IDENTIFYING KEY CONTRIBUTIONS 112
2.10 IDENTIFYING NECESSARY ELEMENTS FOR THE CDFIPM 115
2.11 SUMMARY OF THE CHAPTER 117

CHAPTER 3: DESIGN AND DEVELOPMENT **118**

3.1 INTRODUCTION 118
3.2 THE CENTRAL REQUIREMENTS OF THE CDFIPM 118
3.3 FUNDAMENTALS OF THE CDFIPM 121
3.4 THE PROPOSED MODEL (THE CDFIPM) 127
3.5 READINESS PROCESS CLASS 136
3.6 INITIALIZATION PROCESSES CLASS 138
3.7 ACQUISITIVE PROCESSES CLASS 153
3.8 INVESTIGATIVE PROCESSES CLASS 174
3.9 FUTURE READINESS PROCESS CLASS 195
3.10 OVERRIDING PRINCIPLES 196
3.11 SUMMARY OF THE CHAPTER 207

CHAPTER 4: DEMONSTRATION **208**

4.1 INTRODUCTION 208
4.2 CASE SCENARIO IMPLEMENTATION OF THE CDFIPM 208
4.3 SUMMARY OF THE CHAPTER 239

CHAPTER 5: EVALUATION **240**

5.1 INTRODUCTION 240
5.2 METHODS OF VALIDATION 242
5.3 EXPERT SELECTION PROCESS 244
5.4 EXPERT PANEL MAKEUP 246
5.5 COMMUNICATION AND FEEDBACK FORMATS 250
5.6 EVALUATION QUESTIONNAIRE 252
5.7 FEEDBACK ANALYSIS METHOD 254
5.8 EXPERT FEEDBACK AND ANALYSIS 254
5.9 DISCUSSION OF EVALUATION 272
5.10 ALTERATIONS MADE TO THE CDFIPM 274
5.11 FINAL VERSION OF THE PROPOSED MODEL 282
5.12 ASSESSING THE CDFIPM AGAINST THE THREE CRITERIA 282
5.13 COMPARISON OF THE CDFIPM AGAINST PREVIOUS MODELS 285
5.14 SUMMARY OF THE CHAPTER 294

CHAPTER 6: CONCLUSIONS 295
6.1 INTRODUCTION 295
6.2 COMMUNICATION 295
6.3 RESEARCH SUMMARY 297
6.4 RESEARCH QUESTIONS ADDRESSED 300
6.5 RESEARCH OBJECTIVES ACHIEVED 302
6.6 RESEARCH AIM ACHIEVED 303
6.7 RESEARCH PROBLEM ADDRESSED 304
6.8 RESEARCH CONTRIBUTION 305
6.9 LIMITATIONS AND FUTURE WORK 306
6.10 SUMMARY OF THE CHAPTER 307

REFERENCES 308

APPENDIX A. FORENSIC LABORATORY EXPERIMENTATION 326
A.1 BACKGROUND TO THE CASE 328
A.2 EXECUTIVE SUMMARY 329
A.3 OBJECTIVES 330
A.4 RELEVANT FINDINGS 331
A.5 STEPS TAKEN 343
A.6 TIMELINE OF IMPORTANT EVENTS 352
A.7 CONCLUSIONS 354
APPENDIX A1. GLOSSARY OF TERMS 355
APPENDIX A2. CASE DOCUMENTS 356

APPENDIX B. FINAL VERSION OF THE PROPOSED MODEL 358
B.1 THE CDFIPM'S ABSTRACT REPRESENTATION 358
B.2 THE CDFIPM'S UML ACTIVITY DIAGRAMS 359

List of Publications

1) Montasari, R (2016). 'An Ad Hoc Detailed Review of Digital Forensic Investigation Process Models', *International Journal of Electronic Security and Digital Forensics (IJESDF),* 8 (3), pp. 205-223.

2) Montasari, R (2016). 'A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensics Practice', *International Journal of Computer Science and Security (IJCSS),* 10 (2), pp. 69-87.

3) Montasari, R. (2016). 'A Comprehensive Digital Forensic Investigation Process Model', *International Journal of Electronic Security and Digital Forensics (IJESDF),* 8 (4), pp. 285-301.

4) Montasari, R. (2016). 'Review and Assessment of the Existing Digital Forensic Investigation Process Models', *International Journal of Computer Applications,* 147 (7), pp. 41-49.

5) Montasari, R., Peltola, P. and Carpenter, V. (2016). 'Gauging the Effectiveness of Computer Misuse Act in Dealing with Cybercrimes', *International Conference on Cyber Security and Protection of Digital Services,* pp. 1-5.

6) Montasari, R., Peltola, P. and Evans, D. (2015). 'Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 83-95.

7) Montasari, R. and Peltola, P. (2015). 'Computer Forensic Analysis of Private Browsing Modes', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 96-109.

8) Montasari, R. (in press). 'Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction', *Proceedings of 11th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*.

9) Montasari, R. (in press). 'A Standardized Data Acquisition Process Model (SDAPM) for Digital Forensic Investigations', *International Journal of Information and Computer Security (IJICS)*.

List of Figures

Figure 1. The DSRP model after Peffers et al. (2006) ... 19
Figure 2. The FDFS after Palmer (2001) ... 50
Figure 3. The IDIP after Carrier and Spafford (2003) ... 59
Figure 4. The EDIPM after Baryamureeba (2004) ... 61
Figure 5. The EMCI after Ciardhuáin (2004) ... 63
Figure 6. The HOBFDIP after Beebe and Clark (2005) ... 67
Figure 7. The FSFP after Kent et al. (2006) ... 69
Figure 8. The FDFI after Kohn et al. (2006) ... 71
Figure 9. The CFFTPM after Rogers et al. (2006) ... 73
Figure 10. The CPMIRCF after Freiling and Schwittay (2007) ... 77
Figure 11. The TDERAPM after Khatir et al. (2008) ... 79
Figure 12. The GCFIM after Yusoff et al. (2011) ... 86
Figure 13. The SDFIM after Agarwal et al. (2011) ... 87
Figure 14. The hierarchical structure of the CDFIPM's components ... 127
Figure 15. The abstract representation of the CDFIPM ... 129
Figure 16. The Readiness, Incident Detection and First Response Processes ... 130
Figure 17. The Planning and Preparation Processes ... 131
Figure 18. The Secure and Evaluate Crime Scene and Identification Processes ... 132
Figure 19. The Acquisition and Collection Process ... 133
Figure 20. The Examination, Analysis, Interpretation, Event Reconstruction and Reporting Processes 134
Figure 21. The Presentation, Investigation Closure and Future Readiness Processes ... 135
Figure 22. The UML Activity Diagram of the Readiness Processes ... 137
Figure 23. The UML Activity Diagram of Initialization Class Processes in their abstract level ... 138
Figure 24. The UML Activity Diagram of the Incident Detection Process ... 139
Figure 25. The UML Activity Diagram of the First Response Process ... 142
Figure 26. The UML Activity Diagram of the Planning Process ... 145
Figure 27. The UML Activity Diagram of the Preparation Process ... 152
Figure 28. The UML Activity Diagram of Acquisitive Class Processes in their abstract level ... 153
Figure 29. The UML Activity Diagram of the Secure and Evaluate Crime Scene Process ... 155
Figure 30. The UML Activity Diagram of the Identification Process ... 162
Figure 31. The UML Activity Diagram of the Acquisition and Collection Process ... 169
Figure 32. The UML Activity Diagram of Investigative Class Processes in their abstract level ... 174
Figure 33. The UML Activity Diagram of the Examination Process ... 176
Figure 34. The UML Activity Diagram of the Analysis Process ... 180
Figure 35. The UML Activity Diagram of the Interpretation Process ... 183
Figure 36. The UML Activity Diagram of the Event Reconstruction Process ... 185
Figure 37. The UML Activity Diagram of the Reporting Process ... 187
Figure 38. The UML Activity Diagram of the Presentation Process ... 189
Figure 39. The UML Activity Diagram of the Investigation Closure Process ... 192
Figure 40. The UML Activity Diagram of the Future Readiness Process Class ... 195
Figure 41. Evaluation Questionnaire ... 253
Figure 42. The modified version of the abstract representation of the CDFIPM ... 275
Figure 43. Amendment to the CDFIPM for ALT #2, DEL #1 and ADD #1 ... 276
Figure 44. The CDFIPM's Planning and Preparation Processes, no amendment required ... 277
Figure 45. Amendment to the CDFIPM for ALT #1, ADD #2 and DEL #2 & #3 ... 278
Figure 46. The CDFIPM's Acquisition and Collection Process, no amendment required ... 279
Figure 47. Amendment to the CDFIPM for ADD #6 & #7, ALT #3 & #5 and DEL #4 ... 280
Figure 48. Amendment to the CDFIPM for ALT #4, #6, #7 & #8 and ADD #8 ... 281
Figure 49. The suspect's "C:\WINNT\system32\config\system" registry hive loaded for investigation 335
Figure 50. Entries of Bo2k found on "downloads.sqlite" ... 341
Figure 51. Log file of the original image ... 343
Figure 52. Original given HD image verified again through MD5 and SHA1 checksums ... 345
Figure 53. Raw image format verified through corresponding MD5 and SHA1 checksums ... 345
Figure 54. Avast anti-virus classifying B2OK as a Trojan program and blocking its opening ... 346
Figure 55. The 'dxdiag.exe' examined inside VMware Player and found to be spyware ... 347
Figure 56. B2OK file browsed and scanned using VirusTotal ... 347
Figure 57. The result of the scan showing B2OK as a Trojan program with high detection ratio ... 348

Figure 58. The deleted files in the recycler 349
Figure 59. DC3.zip pointing to the previously downloaded B2OK program 349
Figure 60. The paths to the INFO files: the INFO2 pointing to the "Recycler" deleted folder 350
Figure 61. Analysis of "INFO2" in "rifiuti" revealing no further information 350
Figure 62. Timeline of items of evidence 352
Figure 63. Timeline of web history and downloads 353
Figure 64. Timeline of installed programs 353
Figure 65. Final version of the CDFIPM's abstract representation 358
Figure 66. Final version of the Readiness, Incident Detection and Intelligence Gathering Processes 359
Figure 67. Final version of the Planning and Preparation Processes 360
Figure 68. Final version of the First Response Process 361
Figure 69. Final version of the Acquisition and Collection Process 362
Figure 70. Final version of the Examination, Analysis, Interpretation, Event Reconstruction and Reporting Processes 363
Figure 71. Final version of the Presentation, Investigation Closure and Future Readiness Processes 364

List of Tables

Table 1. The comparative summary of the existing DFIPMs 108
Table 2. Scores obtained by the previous models based on the three assessment criteria 111
Table 3. Mapping the previous models to the proposed model 286
Table 4. Factual evidence item 1: text file 331
Table 5. Factual evidence item 2: image file 332
Table 6. Factual evidence item 3: database file 333
Table 7. Factual evidence items 4 and 5: a desktop shortcut and a database file 334
Table 8. Factual evidence item 6: executable file- an SFTP client for Microsoft Windows 335
Table 9. Factual evidence items 7: registry data- WinSCP CDCache 336
Table 10. Suspicious evidence item 1: MSN instant messages saved as XML file 338
Table 11. Suspicious evidence item 2: doc file 339
Table 12. Suspicious evidence items 3, 4, 5, 6 and 7: five PDF files 340
Table 13. Suspicious evidence item 8: Back Oriface 341
Table 14. Suspicious evidence item 9: executable file- SchedulingAgent 342
Table 15. Evidence record document 356
Table 16. Hard drive image document 357
Table 17. Job request document 357

List of Abbreviations

ACPO	=	Association of Chief Police Officers
CDFIPM	=	Comprehensive Digital Forensic Investigation Process Model
CMA	=	Computer Misuse Act
DEFR	=	Digital Evidence First Responder
DFA	=	Digital Forensic Analyst
DFI	=	Digital Forensic Investigation and Digital Forensic Investigator
DFIPM	=	Digital Forensic Investigation Process Model
DFL	=	Digital Forensic Laboratory
DFP	=	Digital Forensic Practitioner
DFRWS	=	The First Digital Forensic Research Workshop
DSR	=	Design Science Research
DSRP	=	Design Science Research Process
FLM	=	Forensic Laboratory Manager
FRE	=	Federal Rules of Evidence
HTCU	=	High Tech Crime Unit
ISP	=	Internet Service Provider
NIST	=	National Institute of Justice
PDA	=	Personal Digital Assistants
PED	=	Personal Electronic Devices
RIPA	=	Regulation of Investigatory Powers Act

Declaration

I certify that this thesis is the result of my own independent investigation and has not been submitted for any other degree at this or any other university. The views expressed in the thesis are my own.

Signed: Reza Montasari Date: 27th June 2016

Abstract

Nowadays, as a result of the ubiquitous nature of information technology, evidence presented in court is less likely to be on paper. Evidence of computer crime also differs from that related to traditional crimes for which there are well established standards and procedures. In order for digital evidence to be admissible, investigators need to demonstrate that they have specialised knowledge and have applied reliable principles and models to acquire it. Careful notice is taken in court of the manner in which the digital investigative process has been carried out. However, despite such requisites, the field of digital forensics still lacks formal process models that courts can employ to determine the reliability of the process followed in a digital investigation. The existing models have often been developed by digital forensic practitioners, based on their own personal experience and on an ad-hoc basis, without attention to the establishment of standardisation within the field. This has prevented the institution of the formal processes that are urgently required. Moreover, as digital forensic investigators often operate within different fields of law enforcement, commerce and incident response, the existing models have often tended to focus on one particular field and have failed to consider all environments. This has hindered the development of a generic model that can be applied in all the different fields of digital forensics. In addition, the existing models often capture only one part of the investigative process as opposed to the entire process. To address these shortcomings, this research makes a novel contribution by proposing a Comprehensive Digital Forensic Investigation Process Model (the CDFIPM), encompassing the entire digital investigative process, which is formal[1] in that it synthesizes, harmonises and extends the existing models, and which is generic in that it can be applied in the three stated fields of digital forensics.

[1] In the context of this thesis, the term 'formal' is not equivalent to the same term employed in the domains of Mathematics and Computer Science, in which the word 'formal' is used to refer to a set of strings of symbols that might be constrained by rules that are specific to it. In contrast, for the purposes of this thesis, the term 'formal' has been employed to refer to the UML Activity Diagrams, scientific methods, standards of practice, consistency, structure, agreed-upon components and terminology, harmonisation, and the unified approach that have been brought to the proposed model, the CDFIPM.

The methodology used to carry out this research is the Design Science Research widely adopted in the domain of Information Systems on the basis that it is suitable for the design and development of novel artefacts and the analysis of the performance or use of such artefacts. The Peffers et al's (2006) Design Science Research Process model is followed during the course of this research as the appropriate selection of the Design Science Research on the basis that it is inclusive of the common elements of the previous Design Science Research studies.

Existing models are critically reviewed and assessed against three different assessment criteria including: Beebe and Clark's four-point requirement, Carrier and Spafford's five-point requirement and the Daubert Test. The result of the model assessment reveals that there does not exist a model that has all the three characteristics of being "comprehensive", "formal" and "generic". However, through the model assessment, some models are identified that can contribute to the design and development of the proposed model. Following identification of the prevailing models, their key contributions are determined based on the assessment criteria, and the necessary components for the new model are then identified. A new set of domain-specific components is then developed in addition to the already identified components. Following identification of the necessary components and the newly developed set of domain-specific components, the outcome of the design and development stage is the proposed Comprehensive Digital Forensic Investigation Process Model, the stages of which are represented through the use of the UML Activity Diagrams. Based upon the selected methodology (the DSRP), the CDFIPM is tested through both the Demonstration and Evaluation activities. The Demonstration activity involves applying the model into various cases studies and performing a walkthrough of the model, as well as conducting a forensic laboratory experimentation. The Evaluation stage involves the independent verification and validation of the model by its intended user community, including digital forensic investigators operating within the three fields of relevance for this research, namely law enforcement, commerce and incident response, as well as experts in the domain of digital forensics, legal practitioners, a judge and researchers in both academia and industry. After feeding the results of the Evaluation stage back into the CDFIPM's design and development stage, the model is amended accordingly.

Acknowledgments

The journey of my PhD has been both humbling and exciting. I am extremely grateful to my Heavenly Father and the Lord, Jesus Christ, for sustaining me throughout the progression of my thesis, despite many challenges. Without the Father's loving grace, I would have never been able to complete this research.

There are so many people I would like to thank for their kind support of both myself and my research. Firstly, my special gratitude goes to my Director of Study, Dr. Victoria Carpenter, who became very dear to me from the outset of my PhD. She kept a sense of humour when I had lost mine, and her care and selfless giving of her time were sometimes all that kept me going. Victoria's extensive knowledge in research and her experience in managing a PhD student played a significant role in advancing the completion of this research. I am also indebted to my supervisor, Dr. David Evans, whose attention to detail encouraged me to apply critical thinking to this study. David sadly passed away just before the submission of my PhD. He will be greatly missed, as will our scholarly conversations over a good pint of real ale. I am also grateful to my other supervisor, Professor Richard Hill, for so much helpful advice in relation to both my academic performance and my development as a researcher. His support for my research extended to facilitating the funding for me to attend conferences in my field. My thanks also go to the Department of Computing and Mathematics for the trust placed in me to undertake this PhD.

The kind involvement of a number of experts has greatly assisted me in completing this study. In particular, I would like to express my thanks to six people who made it possible to accomplish my PhD: (1) Criminal Law Barrister, Rebecca Griffiths of Apex Chambers in Cardiff; (2) Chairman of the Northern Chancery Bar Association and a Trustee of the North West Partnership, Mark Cawson, a Deputy High Court Judge of Exchange Chambers in Manchester, Leeds and Liverpool; (3) Detective Sergeant Andrew Dodd from the High-Tech/Cyber Crime Team of the North West Regional Organised Crime Unit (TITAN); (4) Detective Sergeant Karl Fenny from Cheshire Police Headquarters High-Tech Crime Unit; (5) Detective Constable Tim Williams from Gwent Police High-Tech Crime Unit; and (6)

Mark Maybiy from Gwent Police. Without all of their feedback, this study would not have been completed. I would like to thank Richard Brian Adams, whose study "The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice" has inspired and influenced this study. Pekka Peltola, my friend and a PhD colleague, has been very supportive during my PhD. So, thank you Pekka.

I would also like to thank my best friends, Rowland and Becky for going through the ups and downs of my PhD. Thank you both for your patience and kindness. I am also very grateful to the rest of my church family in Nottingham for their support, encouragement and prayers during this process. Without your loving support, I would have found it very difficult to settle into a new life in Nottingham and my PhD study. Finally, I thank my parents, Lohrasb and Zeinab, and my brothers and sister, Farshad, Hooman and Helen, for their love and encouragement throughout.

Chapter 1: Introduction

In this Chapter, three issues associated with the existing digital forensic investigation process models (DFIPMs) will be identified. The three problems relate to the lack of a model that has all the three characteristics of being "comprehensive", "formal" and "generic". These three issues will be formulated into one single key research problem as follows:

> *That there does not exist a comprehensive model encompassing the entire digital investigative process that is formal such that it can assist courts of law in determining the reliability of the investigative process followed, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response (Montasari, 2016, c).*

Therefore, a Comprehensive Digital Forensic Investigation Process Model (the CDFIPM) is proposed, encompassing the entire investigative process. It is formal in that it synthesizes, harmonises and extends the existing models (see the footnote in page x or the section 1.4.1 for the meaning of the term 'formal' in the context of this study) and generic in that it can be applied in the three fields of law enforcement, commerce and incident response. By implementing the CDFIPM, this model will be of immediate value to both digital forensic investigators (DFIs) operating within the stated fields and courts of law. Moreover, as Adams (2012) state, the development of such a model will establish a starting point from which other investigators and researchers in the field will be able to continue to advance the field's scientific credentials. Following the identification of the research problem, this chapter will proceed to define the research hypothesis, aim, objectives, questions, scope, limitation, contributions and methodology, concluding with a summary.

1.1 Background

Nowadays, the nature of evidence presented in courts of law is less likely to be paper-based due to the ubiquitous nature of information technology (Adam, 2012; Stanfield, 2009). Evidence of computer crime differs from that related to traditional crimes for

which there are well established standards and procedures (Adams, 2012; Stanfield, 2009; Smith et al., 2011). In order for digital evidence to be admissible, investigators need to demonstrate that they have specialised knowledge, and that the evidence was acquired using reliable principles and methods (Kessler, 2010). As with other types of evidence, digital evidence is not assumed to be valid and reliable: empirical testing in relation to the theories and techniques of its production is required (Adams, 2012; Mason, 2007). Careful notice is taken in court of the manner in which the digital investigative process has been carried out (Cohen, 2011; Kessler, 2010; Mason, 2007).

A digital forensic investigator might discover significant and incriminating evidence, but if they cannot present the evidence in a coherent and understandable way to the lay audience (such as judge and jury), the case may be lost (Sherman, 2006). The complexity of tools and methodologies used to perform a digital investigative process requires investigators to be able to explain the process in a manner that a judge and jury can understand it (Kessler, 2010). Such tools and methodologies must also adhere to some standards of practice and be accepted by other investigators operating in the field (Adams, 2012; Kessler, 2010; Armstrong, 2010).

Nevertheless, the field of digital forensics still lacks both consensus and formal process models that the courts can employ to determine the reliability of the digital evidence presented to them (Montasari et al., 2015; Valjarevic and Venter, 2015; Kohn et al., 2013, US-CERT, 2012; Agarwal et al., 2011). This lack of a formal model is not an isolated flaw within the field of digital forensic science. Cohen (2012) states that the entire field of digital forensic still lacks consensus in fundamental areas. A study conducted by Cohen et al. (2011) on the level of consensus in foundational elements of digital investigative process revealed the lack of use of common definitions and language. The authors state that the consensus can be found only after the definitions are made explicit (Cohen et al., 2011). The absence of agreements associated with DFIPMs has also been widely acknowledged also by other researchers (Montasari, 2016, c; Valjarevic and Venter, 2015; Adams et al., 2014; Kohn et al., 2013; Agarwal et al., 2011; Rogers et al., 2006). Zainudin et al. (2011) state that one of the most significant problems encountered by digital forensic investigators is the absence of standardisation in the field of digital forensics.

Casey (2011) argues that the development of a formal process model enables a complete, rigorous investigation, ensures proper evidence handling and reduces the chances of mistakes created by preconceived theories, time pressures, and other potential pitfalls (Casey, 2011). Similarly, Valjarevic and Venter (2015) state that conducting a digital forensic investigation requires a formalized process model, arguing, "There is currently neither an international standard nor does a global, harmonized DFI process (DFIP) exist". Montasari et al. (2015) and Trcek et al. (2010) suggest the concept of a widely agreed-upon process model to harmonise the practice of digital forensics. However, despite many calls to bring formalisation to DFIPMs, a solution has not yet been provided (Valjarevic and Venter, 2015; Adams et al., 2014; Kohn et al., 2013; Cohen, 2012). Many researchers, also as cited by Adams (2012), acknowledge the limited progress, if any, in defining and improving a formal digital forensic process since the DFRWS held in 2001 (Montasari, 2016, a; Montasari et al., 2015; Cohen, 2011; Aggarwal et al, 2011; Nance et al., 2009; Trcek et al, 2010).

One reason for the absence of formal process models is the relatively recent addition of digital forensics as a scientific discipline compared to traditional forensic science (Cohen, 2012). The latter has developed, together with its fundamental biological sciences, over several decades (Beebe and Clark, 2005; Palmer, 2001), whereas digital forensic science is still being formed and therefore lags considerably behind the better-developed, underlying computer science (Beebe and Clark, 2005; Carrier et al, 2003). Some researchers argue that the digital forensic discipline has developed without any of the initial research required to provide an essential, thorough, scientific foundation (Valjarevic and Venter, 2015; US-CERT, 2012; Peisert et al., 2008; Meyers and Rogers, 2004; Carrier, 2002).

The United States Computer Emergency Readiness Team (US-CERT, 2012) also acknowledges that digital forensics is still in its infancy, noting, "Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry." Meyers et al. (2004) take an even stronger view, warning that digital forensics is branded as a "junk science" because of the absence of certifications, standards or peer-reviewed methods (Meyers et al., 2004). Similarly, Carrier (2002) highlights that issues are raised in considering digital forensics as a science due to the absence of generally agreed-upon standards and procedures. Having no formal DFIPMs

for the digital investigative process, courts have resorted to applying methods used to test "classical evidence" to determine the reliability of "digital evidence" (Adams 2012; Kessler, 2010; Calhoun, 2008). For instance, in the United States, federal courts apply the Daubert Test to determine the reliability of digital evidence (discussed in detail in Chapter 2).

A further cause of the lack of formal models for digital investigative process is the "ad-hoc" approach taken by the authors of these models, who have failed to employ scientific approaches when developing them. Previous models have often been developed by practitioners based on their own personal experience, on an ad-hoc basis (Montasari, 2016, c; Montasari et al., 2015; Valjarevic and Venter, 2015; Adams, 2012; Aggarwal et al., 2011). This could be because digital forensics is often conducted by practitioners who are not scientists but law enforcement officers (Adams et al., 2012; Mayer et al., 2004). However, Karyda and Mitrou (2007) state that using ad-hoc methods and tools for the extraction of digital evidence can undermine its reliability and credibility. Referring to the same issue, Reith et al. (2002) state, "This is a problem because evidence must be obtained using methods that are proven to reliably extract and analyse data without bias or modification (Reith et al., 2002)." This is further supported by Beebe and Clark, who argue that rigor in a DFIPM is achieved only through the use of "formal" and "scientific" approaches (Beebe and Clark, 2005), and by Solomon et al. (2011), who argue that current procedures and tools should not be mistaken for a consistent investigative process. The latter authors contend,

> *Tools and procedures are developed from the experience of law enforcement and system administrators simply in an ad-hoc manner rather than "coming from the scientific community where other traditional forensic sciences get their methodologies" (Solomon et al., 2011).*

In conclusion, the adoption of ad-hoc approaches in developing previous models has led to a variety of process models with conflicting stages, activities and terminology, which in turn has prevented the establishment of the formal processes urgently needed by courts and investigators alike (Montasari et al, 2015; Adams, 2012; Agarwal et al., 2011). As a result, many researchers have increasingly called for scientific approaches and formal methods for the digital investigative process (Cohen, 2012; Carlton and Worthley, 2009; Garfinkel et al, 2009; Pollitt, 2009; Leigland and Krings, 2004).

A further issue with the existing models is their tendency to focus on one specific area of digital forensics, neglecting other environments (Montasari, 2016, b and c; Montasari et al., 2015). Unlike in other domains of forensic practice, digital forensic investigators operate in various fields (Adams, 2012; Freiling, 2007; Beebe and Clark, 2005; Ciardhuáin, 2004). Therefore, as Carrier and Spafford (2003) argue, "A model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response." However, instead of being generic, previous models have often focused on only one specific area, such as law enforcement, commerce or incident responses (Adams, 2012, Pollit, 2009), therefore failing to consider the requirements of those operating in different domains. The result has been the hindering of the development of a generic model that can be applied in the various fields of digital forensics (Montasari, 2016, a, b and c; Montasari et al., 2015).

A third significant concern associated with the previous models is that they are not comprehensive, failing to cover the entire investigative process. The models often focus on the "middle part" of the investigative process, that being 'Identification, Acquisition and Examination Processes,' excluding other essential stages (see Chapter 2). Beebe and Clark argue that a more comprehensive and generally accepted framework is needed to enhance scientific rigor and facilitate education, application and research (Beebe and Clark, 2005). Similarly, Ciardhuáin states,

> *A comprehensive model of cybercrime investigations is important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators. (Ciardhuáin, 2004)*

However, as of May 2016, such a comprehensive model is not found in the current literature (see Chapter 2). Although a few researchers have attempted to capture the entire investigative process in their models (Valjarevic and Venter, 2015; Kohn et al., 2013; Aggarwal et al., 2011), they tend to be predominantly single-tier, higher order process models, focusing on the abstract, rather than the more concrete principles of the investigation. Beebe and Clark (2005) supported by Montasari (2016, c) and Kohn et al. (2006) criticise this approach, arguing that the complexities of the digital investigative process cannot be represented at such a high level. Beebe and Clark develop their point with an analogy, stating that if flying an airplane were a function of

a higher order framework consisting of three phases: "take-off", "fly" and "land", very few pilots could achieve the task without acquiring further details in relation to each phase. In the same way, greater detail for each stage of a digital investigative process is required in order to enhance the usability of the forensic methodology for DFIs (Beebe and Clark, 2005). Such detail is missing in the existing DFIPMs.

1.2 Research Problem

The foregoing considerations lead to the following research problem[2]:

> *There does not exist a comprehensive model encompassing the entire digital investigative process that is formal, such that it can assist a court of law in determining the reliability of the investigative process followed, and that is generic, in that it can be applied in the different fields of law enforcement, commerce and incident response.*

1.3 Research Hypothesis

1.3.1 Hypothesis 1

A formal process model can be developed that is comprehensive in that it encompasses the whole digital forensic process and that is generic in that it can be employed by the digital forensic investigators in the fields of law enforcement, commerce and incident response.

1.3.2 Hypothesis 2

A formal process model will enable digital forensic investigators to carry out more effective, forensically-sound digital investigations than is possible with the use of ad-

[2] The research problem is also influenced by Adams (2012) study, which calls for other researchers "... *to provide a more comprehensive model. Ultimately the other activities of digital forensic practitioners (such as analysis and presentation) could be incorporated in the same format in order to provide a complete formal model of digital forensics.*" See section 7.7.2 of Adams' (2012) study.

hoc tools, and will assist the courts in determining the reliability of the processes employed in such investigations.

1.4 Research Aim, Objectives and Questions

1.4.1 Research Aim

The aim of this research is to develop a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonises and extends the existing models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response.

In the context of this thesis, the term 'formal' is not equivalent to the same term employed in the domains of Mathematics and Computer Science, in which the word 'formal' is used to refer to a set of strings of symbols that might be constrained by rules that are specific to it. In contrast, for the purposes of this thesis, the term 'formal' has been employed to refer to the UML Activity Diagrams, scientific methods, standards of practice, consistency, structure, agreed-upon components and terminology, harmonisation, and the unified approach that have been brought to the proposed model, the CDFIPM.

1.4.2 Research Objectives

In order to achieve the aim, the following objectives must be accomplished:

1. Critically analyse and assess the previous DFIPMs against different assessment criteria in order to identify the models that can contribute to the design and development of the new model.

2. Following the identification of the prevailing models (those that have withstood the assessment), determine their key contributions based on the assessment criteria.

3. Identify the components essential for the new model from a combination of the key contributions of both the prevailing and the reviewed models.

4. Build upon the contributions of the previous models by constructing a new set of domain-specific components.

5. Based upon the above preceding steps, design and develop a formal representation of the new model (the term "formal" is defined both in abstract and also under the research aim, section 1.4.1), incorporating both the identified components and the new set of constructed components.

6. Evaluate the model using three methods, including applying the model to different case studies, assessing it against the different assessment criteria used to assess the previous models and recruiting different sets of independent experts.

1.4.3 Research Questions

In order to achieve the research objectives, the following three research questions, inspired by Adams' (2012) study, need to be answered:

1. What are the essential components necessary in a comprehensive model that is formal, generic and forensically sound for the entire digital forensic process?

2. Once the components of such a comprehensive model that is formal, generic and forensically sound are determined, how can they be integrated into a working model?

3. What is the most appropriate method to describe, present and use the model for the entire digital forensic process?

To answer these questions, this research will enable the design and development of a forensically sound and comprehensive model, the CDFIPM, encompassing the entire digital forensic process. It will be formal in that it synthesizes and extends the existing

models, and generic in that it can be employed in the different environments of digital forensics. It is contended that the CDFIPM will be a significant step towards instituting the currently lacking standards which would assist in establishing an improved digital forensic investigative process.

1.5 Scope, Limitations and Assumptions

1.5.1 Environmental and Jurisdictional Scopes

The environment scope for this research has been limited to the three fields of "law enforcement", "commerce" and "incident response" digital forensic practice within the United Kingdom jurisdiction. The military environment has not been considered due to the fact that it is difficult for anyone outside of this area to acquire data on their processes, as Adams (2012) states. The jurisdiction is limited to the United Kingdom due to the difficulty of assessing the model against the requirements of a large number of jurisdictions where digital forensics are carried out (Adams, 2012). Making the model appropriate for other jurisdictions could be an aspect of future research. However, it is contended that the CDFIPM, as it stands, has relevance to other jurisdictions with similar legal foundations for evaluating the digital investigative process.

1.5.2 Digital Forensics Branch Scope

The proposed model focuses predominantly on "Computer Forensics" as opposed to any other branches of digital forensics such as Malware Forensics, Cloud Forensics, Network Forensics or Mobile Forensics. Although some much simpler models (Valjarevic and Venter, 2015; Aggarwal et al., 2011; Freiling and Schwittay, 2007) have claimed to be appropriate for various branches of the digital forensics, such a claim is not made in relation to the CDFIPM for accuracy purposes. However, due to the CDFIPM's generic steps and activities, it could be easily adapted to cover any of the stated branches. The CDFIPM therefore provides guidance mainly for the following types of digital devices used in different circumstances:

- Digital storage media used in standard computers such as hard drives, optical and magneto optical disks and data devices with similar functions;
- Desktop and laptop computers with network connections;
- Digital still and video cameras, Tablets, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), removable storage media, and memory cards; and
- Devices with similar functions to the above.

1.5.3 Types of Audience Scope

The research presented in this thesis is aimed at digital forensic investigators in the three domains of law enforcement, commerce and incident response, as well as judges and legal practitioners. The research is also relevant to the research community of digital forensics and information security. For reasons of simplicity, the term "Digital Forensic Investigators (DFIs)" is used throughout this research to refer to different digital forensic personnel including the "Digital Forensic Practitioners (DFPs)", "Digital Forensic Analysts (DFAs)", "Digital Evidence First Responders (DEFRs)", and "Forensic Laboratory Managers (FLMs)".

1.5.4 Details Scope

The success of each step of the investigative process is dependent upon 'Forensic Readiness' in the form of policies, protocols, procedures, training and experience (Kohn et al., 2013; Casey, 2011; Rowlingson, 2004). An investigating organisation employing the CDFIPM must therefore already have their own standard operating procedures (SOPs) in place, in which methodologies are already defined and appropriate procedures have already been developed. The CDFIPM is intended to assist investigating organisations in structuring their existing methods in a formal manner that can be easily described to the courts, as opposed to replacing them completely, an approach supported by Adams (2012). It would be impractical to attempt to provide specific guides in relation to different technologies as any specific method can easily become obsolete in light of the constant and rapid changes in technology (Adams, 2012). Specific methods in relation to new domains of technology can be found in

research and technical papers which are frequently being updated. They can help investigators with new or unfamiliar technology and best practices (Adams, 2012; Sammes and Jenkinson, 2007). It is therefore outside the scope of this research to provide the investigating organisation with techniques or methods of digital forensic investigation.

1.5.5 Assumptions

It is assumed that those investigators who follow the CDFIPM have the essential skills, training and experience for conducting digital forensic investigations. However, due to its detailed approach, the CDFIPM also could provide valuable proper training to inexperienced investigators. In accordance with ISO/IEC 27043 (2015) and ISO/IEC 27037 (2012), it is also assumed that DFIs using the CDFIPM will have obtained proper authorisation prior to initiating the digital investigation, and that they will adhere to the requirements that their actions are:

- auditable through proper documentation;
- repeatable in that using the same tools on the same item under the same conditions would produce the same results;
- reproducible in that employing different tools on the same item would produce substantially similar results;
- and justifiable.

In accordance with ACPO (2012), it is also assumed that investigating organisations employing the CDFIPM will adhere to the following four principles to optimise the admissibility of the digital evidence in the United Kingdom courts:

- Principle 1: No action taken by investigators should change any data which may subsequently be relied upon in court.
- Principle 2: In circumstances where an investigator finds it necessary to access original data, that person must be competent to do so and able to give evidence explaining the relevance and implications of their actions.

- Principle 3: An audit trail or other record of all processes applied to the digital evidence should be created and preserved. An independent third party ought to be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation has overall responsibility for ensuring adherence to the law and these principles.

Furthermore, due to rapid technology changes, this research does not take into account the use of particular tools or methods, an approach supported by Adams (2012). However, an assumption is made that DFIs employ only tools that have been approved in courts of law, such as FTK, EnCase or X-Ways.

1.6 Research Contribution

This research makes a significant and novel contribution to the field of digital forensic science by implementing a process model, the CDFIPM, that would assist DFIs in following a uniform approach, and also courts of law in determining the reliability of the processes followed in a digital investigation. The research presented in this paper synthesizes, harmonises and builds upon existing models to produce the first process model with all three characteristics of being "comprehensive", "formal" and "generic". The CDFIPM is represented using formal modelling language, through UML Activity Diagrams, and contains generic methods that DFIs can use to convey technology to non-technical observers. This thesis also contains the most comprehensive, critical review and assessment of all existing digital investigation process models presented, as at May 2016.

1.7 Methodology

This section presents the methodology that has been used in this research. The Design Science Research (DSR), widely adopted in the domain of Information Systems (IS) (Hevner et al., 2010; Peffers et al., 2006; Hevner et al., 2004; March and Smith, 1995; Walls et al., 1992; Nunamaker et al., 1990), has been selected as the methodology to conduct this research. The DSR is used to serve as "the archival venue of science-based design knowledge across multiple disciplines" (Design Science Journal, 2016).

Researchers in the Information Systems domain have used the DSR in their discipline, arguing the validity of Design Science (DS) as an IS research paradigm (Hevner et al, 2010; Edirisuriya, 2009; Peffers et al, 2006; Hevner et al, 2004; March and Smith, 1995; Walls et al. 2004 and 1992; Nunamaker et al., 1990).

The DSR has also been adopted in various other fields, including: Engineering (Fulcher and Hills, 1996; Reich, 1994; Eekels and Roozenburg, 1991; Archer, 1984), Computer Science (Takeda et al. 1990), Software Engineering (Frey, 2013) and the Business Model Ontology (Osterwalder, 2004). In addition, the DSR has been used for the first time in the domain of digital forensics in a research study conducted by Adams (2012). The main aim of the DSR is to achieve or develop knowledge and understanding of a problem domain by building and applying a designed artefact (Hevner et al., 2004; Aken and Ernst, 2005). The DSR involves the design of novel or innovative artefacts and the analysis of the performance or use of such artefacts (Watts et al., 2009; Kuechler and Vaishnavi, 2008). The development and evaluation of artefacts form an important part in the DSR (March and Storey, 2008; Hevner et al, 2004). Artefacts include, amongst others: models, methods, constructs, instantiations and design theories (March and Smith, 1995; March and Storey, 2008), social innovations, and new or previously unknown properties of technical, social or informational resources (March and Storey, 2008).

The artefact related to this research is a new model, a Comprehensive Digital Forensic Investigation Process Model (CDFIPM), that encompasses the entire digital investigative process. The organisational context associated with this research is that of law enforcement, corporates and incident response. This research also addresses the hitherto unsolved problem that there does not exist a comprehensive model encompassing the entire digital investigative process that is both formal, in that it synthesizes, harmonises and extends the existing models, and generic, in that it can be employed in the different fields of law enforcement, incident response and commerce.

1.7.1 Justification for Using DSR

The selection of the DSR over other research methodologies such as the Grounded Theory (GT) or Requirements Engineering (RE) has not been due to the unawareness of

those methodologies (see sub-sections 1.7.1.1 and 1.7.1.2). The selection of the DSR over other alternative methodologies is justified as it is particularly suited to the task of creating and evaluating a new process model (an IT artefact) (Adams, 2012). Armstrong and Armstrong (2010) state that with the DSR's focus on designing solutions, it is ideal when approaching the problem domain of digital forensics. Hence, because this study also has at its focus the design, development and subsequent evaluation of the CDFIPM, the DSR is considered to be the most appropriate choice. The DSR is also preferable as it is more pragmatic than alternatives such as Explanatory Science Research (ESR) (Aken and Ernst, 2005) and as it can be used to solve a problem for which no solution has already been found (Peffers et al, 2006; Hevner et al, 2004). Therefore, since this research is a problem-based study[3], again the DSR is the most appropriate methodology. Moreover, the DSR uses both inductive and deductive process. Since this study is aimed at producing a new knowledge and literature (through inductive process), as well as testing the two research hypothesises (through the deductive process), once again the DSR is the most appropriate choice.

As stated above, prior to the selection of the DSR as the preferred methodology, the 'GT' and 'RE' were also considered. However, the two stated research methodologies were deemed inappropriate to be adopted in this study. The following two sub-sections briefly discuss the GT and RE and provide the rationale why they were not employed in the study.

1.7.1.1 Grounded Theory

Grounded Theory is a qualitative research methodology employed in early studies in a new field (Kessler, 2010; Leedy and Ormrod, 2010). Although various approaches to Grounded Theory studies have been described in the literature (Charmaz, 2006; Schram, 2006; Dick, 2005; Elliott and Lazenbatt, 2005; Pogson et al., 2002; Brown et al., 2002), these approaches often use five similar fundamental components as follows:

[3] This research aims to address the problem that there does not exist a Comprehensive Digital Forensic Investigation Process Model (CDFIPM) that is both formal and generic.

- **Data Collection**: Grounded Theory research begins with basic data collection, usually using open-ended questions in the form a questionnaire or interview.

- **Note Taking:** As data are collected, the researchers must take note of the emerging themes.

- **Coding**: In order to compare the data provided by the different study participant and detect emerging trends, data are coded at this stage through both 'initial coding' and 'focused coding'.

- **Memoing**: The next stage in the process is to write memos. During this step, the researcher must organise the trends to define categories and relationships. From here, the researcher can produce theories that are published to offer foundational literature.

- **Writing:** The final stage in the grounded Theory process is to publish the results.

While the GT has, to some extent, similarities to the DSR as both are qualitative studies and share some common components (such as communication/writing and data collection), it is nevertheless considered to be an inappropriate methodology to adopt in this study. In contrast with the DSR, that is problem-focused, the GT is not a problem-centred study. In GT, the researcher is not required to identify a research problem prior to the collection of primary data. Hence, this is why the first entry point in the process is "Data Collection", denoting that the researcher already knows what kind of a problem he/she is going to investigate that they are collecting the primary data for. In contrast, in this study a problem needed to be identified, research hypothesis determined, aim and objectives established, and research questions formulated prior to the data collection. Therefore, since, the DSR provides the "Problem Identification and Motivation" as the first entry point in the process, at which the researcher can start the study, the DSR is considered the most appropriate choice.

Moreover, GT employs only 'inductive process' whereby data is collected to develop a theory (Kessler, 2010; Charmaz, 2006; Dick, 2005; Pogson et al., 2002; Schram, 2006). This is in contrast to the deductive process whereby data is collected to test a hypothesis (Kessler, 2010). Since this study is concerned with providing both a new knowledge and also a foundational literature (through inductive process), as well as testing the research hypothesises (through the deductive process), again the DSR is considered the most appropriate methodology as it provides both inductive process and deductive process. Finally, the GT is not concerned with the design, development and subsequent evaluation of artefacts. Therefore, since this study has at its focus the development and evaluation of the proposed model (the CDFIPM), the GT was considered an inappropriate methodology to adopt in this research.

1.7.1.2 Requirements Engineering

Requirements Engineering (RE) is concerned with the process of refining, documenting and maintaining requirements to the sub-fields of Systems Engineering and Software Engineering related to this process. It focuses on the use of systematic and repeatable techniques that ensure the completeness, consistency, and relevance of the system requirements (Sommerville and Sawyer, 1997). RE consists of the following requirements:

- **Requirements Elicitation** is the process of determining, reviewing, documenting, and understanding the user's requirements and constraints for the system.

- **Requirements Analysis and Negotiation** is the process of checking user's requirements and resolving stakeholder conflicts.

- **Requirements Specification** is the process of documenting the user's requirements and constraints clearly in a requirements document.

- **Requirements Verification** is the process of checking that the system requirements are complete, correct, consistent, and clear and that the

documented requirements and models are consistent and meet stakeholder needs.

- **Requirements Management** is the process of managing changes to the requirements as the system is developed and put into place.

Contrary to the GT that is not concerned with the development and evaluation of IT artefacts, the RE has a focus on the systems and software development, making it more relevant to this study than the GT. However, with the RE, the problem (systems or software requirement) is not identified by the developer (who designs and develop the system/software) rather by the requester or client (who understands the problem to be solved by the system/software but does not know how to develop it). The problem addressed by this study and the research artefact (the CDFIPM) needed to be identified and developed by the thesis author himself. Thus, the DSR was considered to be a more appropriate option than the RE. Moreover, although the RE is concerned with the design and development of IT systems, it is not 'specific' to the task of creating a new process model (Adams 2012; Armstrong and Armstrong 2010), whereas the DSR is 'particularly' suited to the design, development and evaluation of a process model. Hence, since the product of this study is a process model, the DSR was once again considered to be a more appropriate option than the RE. Finally, the RE does not have a 'communication' or 'writing' stage as offered by both the DSR and the GT, in which the results of the study must be published to the scientific user community. Therefore, the DSR was once again considered a more appropriate option in this study.

1.7.2 Selection of the Appropriate DSR Methodology

Various researchers both within and outside the IS domain have provided guidance to define the DSR and have described what goals should be followed in its production (Hevner et al, 2010; Wieringa, 2009; Peffers et al, 2006; Vaishnavi and Kuechler, 2004; Hevner et al, 2004; Adams and Courtney, 2004; Rossi and Sein, 2003; March et al. 1995; Walls et al. 1992; Nunamaker et al., 1990; Eekels and Roozenburg, 1991; Takeda et al, 1990; Archer, 1984). These researchers have often proposed various methods, processes or theoretical frameworks to rationalise the DSR studies.

The most prominent methods in relation to the DSR are those proposed by Hevner et al. (2004)[4] and Peffers et al. (2006)[5] in the domain of Information Systems (IS). Hevner et al. (2004) provided a list of seven guidelines to assist IS researchers in conducting, evaluating and presenting the DSR. The seven guidelines are intended to address: (1) Design as an Artefact, (2) Problem Relevance, (3) Design Evaluation, (4) Research Contribution, (5) Research Rigor, (6) Design as a Research Process, and (7) Communication of Research (Hevner et al, 2004). Similarly, Peffers et al. (2006) developed a "mental process model", the Design Science Research Process (DSRP) (Figure 1), for producing and presenting IS research. It comprises six activities, including: (1) Problem Identification and Motivation, (2) Objectives for a Solution, (3) Design and Development, (4) Demonstration, (5) Evaluation, and (6) Communication.

The Peffers et al's (2006) DSRP model would meet the three following objectives:

- Consistency with prior literature;
- Provision of a nominal process model for undertaking the DSR; and
- Provision of a mental model for presenting and understanding the DSR.

Peffers et al. (2006) combined the findings from seven previous influential DSR studies[6] in order to identify common elements for inclusion in their DSRP model. The result of an all-inclusive DSRP model is the reason it has been selected as the appropriate methodology to follow in this research. The Peffers et al's (2006) DSRP model has also been selected over alternatives such as the seven guidelines by Hevner et al. (2004) as it provides a graphical representation of the conceptual process for both carrying out and presenting the DSR. Such a mental model facilitates the application of the DSR and can also assist the thesis author in producing and presenting a high quality DSR that would be accepted as valuable, rigorous and publishable within the field of digital forensics science.

[4] Google search engine shows that this work has been cited 7, 966 times as of October 7, 2016.
[5] Google search engine shows that this work has been cited 313 times as of October 7, 2016.
[6] These notable DSR studies included those carried out by Hevner et al. (2004); Rossi and Sein, 2003; Walls et al. (1992); Nunamaker et al. (1990); Eekels and Roozenburg (1991); Takeda et al (1990) and Archer (1984).

1.7.3 Describing the DSRP Selected for This Research

It is the common components in Peffers et al's synthesis of the previous DSR studies and their sequential order which form the basis for their DSRP model. The result of the integration is a process model with six activities in a nominal sequence, as presented in Figure 1. The sections following Figure 1 provide a brief description of each activity within the DSRP before a description is given of how the DSRP is applied into this research.

Content was removed for copyright reasons.
Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V. and Bragge, J. (2006). 'The Design Science Research Process: A Model for Producing and Presenting Information Systems Research', *1st International Conference on Design Science Research in Information Systems and Technology*, pp. 83-106.

Figure 1. The DSRP model after Peffers et al. (2006)

Activity 1 – Problem Identification and Motivation

Activity one involves defining the research problem to be addressed and justifying the value of the research based on the perceived benefits of the resulting artefact. To accomplish this activity, researchers are required to have knowledge of the state of the problem and the importance of its solution.

Activity 2 – Objectives of a Solution

The second activity involves researchers defining the aims and objectives in relation to the problem to be resolved. They should be deduced rationally from the problem specification. For this activity, researchers need to have knowledge of the state of the problem, as well as current solutions and their efficacy, if any.

Activity 3 – Design and Development

Activity three requires the researchers to create the artifactual solution. As discussed previously, such artefacts can be constructs, models, methods or instantiations (Hevner et al, 2004). Researchers must have theoretical knowledge for this activity, which they can apply in investigating a solution.

Activity 4 – Demonstration

Activity four involves demonstrating the efficacy of the artefact in an environment appropriate to solve the stated problem. This could involve the researchers applying the artefact in experimentation, simulation, a case study, proof or other appropriate activity. The activity requires effective knowledge of how the artefact should be applied in order to solve the problem.

Activity 5 – Evaluation

The fifth activity involves observation and measurement of how effectively the constructed artefact supports a solution to the stated problem. It involves the researchers comparing the objectives of the solution in Activity 2 to the observed results from the application of the artefact in Activity 4. At this stage, if it became evident that the artefact required further design and development, researchers would return to Activity 3 as part of an iterative process.

Activity 6 – Communication

The final activity of Peffers et al's (2006) DSRP model involves communication of the problem and its significance, the artefact, its utility and novelty, the rigor of its design, and its usefulness for other researchers and appropriate audiences such as practising professionals. This requires researchers to have knowledge of their discipline.

1.7.4 Applying the Methodology to the Research Problem

Although Peffers et al's (2006) DSRP is structured in a "nominally sequential order", researchers will not always proceed in a sequential order from Activity 1 through to

Activity 6. The DSRP model provides four possible entry points, at each of which researchers can start their research process, depending on the type of research approach. The focus of this research being the problem that there does not exist a Comprehensive Digital Forensic Investigation Process Model (CDFIPM) that is both formal and generic, it is based on a "problem-centred approach", and as such the entry point in the DSRP is Activity 1. The DSRP's various entry points allow iteration within the research process. The "build and then evaluate loop" might be iterated a number of times before the final design artefact is produced (Markus et al, 2002). This is important as during the Demonstration and Evaluation Phases of this research, the thesis author might need to return to the Design and the Development Phase to make improvements to the artefact (the CDFIPM).

The following sections explain how Peffers et al's (2006) DSRP will be followed during the course of this research. Moreover, since the DSRP does not comprise the low-level details of how a researcher should carry out the activities within the individual stages (Adams, 2012), the following sections will also explain how the thesis author will apply the process in relation to the appropriate methodologies.

Activity 1 – Problem Identification and Motivation

Rocco and Hatcher (2011) state that many research studies start with the identification of a problem or the purpose for engaging the study. Boote and Beile argue that a detailed and sophisticated literature review provides the foundation for "substantial and useful research" (Boote and Beile, 2005). A profound knowledge of the problem addressed by this research will be acquired through a detailed analysis and assessment of the literature related to previous DFIPMs. There are different approaches to literature review, including, amongst others, Systematic Review, Evaluative Review, Exploratory Review, Instrumental Review and Focused Review (Bryman, 2015). In this research, the Evaluative Review in combination with the Systematic Review will be followed, these being more focused on a research question than the alternatives (Adams et al., 2007). Having drawn conclusions from the literature review, the author will be able to formulate the research questions this thesis is intended to answer. Interactions with other experts and the thesis author's own experience in the field of digital forensics will also provide insight into the stated problem.

Activity 2 – Objectives of a Solution

The research aim has been formulated according to the definition of the problem. This approach is supported by Peffers et al. (2006), who state that objectives should be deduced rationally from the problem specification. Therefore, in order to formulate the stated aim, a deep knowledge has been acquired of the state of the problem and its current solution in the form of previously proposed DFIPMs and their efficacy.

Activity 3 – Design and Development

Prior to designing and developing the new model, all previously proposed models will be analysed and assessed against three different assessment criteria[7] (see Chapter 2 for details), in order to identify which can contribute to the model in this research. Law enforcement, commerce and incident response are the three environments on which this research focuses, therefore the existing models within those three domains which most closely meet the assessment criteria will be considered for their possible contributions to the new model. Such an approach is considered important by other researchers (Kohn et al., 2013 and Cohen 2012 and 2010) as any model institutionalized through subsequent intellectual discourse and practical use must take into account other researchers' perspectives, approaches and "vernacular".

In order to assess the previous models against the three sets of assessment criteria, each model will be given three sets of scores in accordance with the three sets of assessment criteria[8]. Models will be scored according to how many of the requirements are met for each particular set of criteria. This method of assessing the previous DFIPMs against "three" different criteria is another novel contribution of this research in the field of digital forensic science. However, this approach should not be considered as a conclusive assessment (Adams, 2012). Rather, the score-based assessment of previous models is employed to determine how many of the requirements of each given criteria have been fulfilled by a model, as closely as is possible (Adams, 2012).

[7] The idea of assessing the existing DFIPMs against the assessment criteria was originally devised by Adams (2012). However, Adams (2012) uses only two sets of assessment criteria.

[8] This denotes that each score given to a model will correspond with a particular set of the assessment criteria. The idea of using score-based approach has been derived from Adams' (2012) study.

Once the most reliable models[9] have been identified, their specific key contributions will be determined for inclusion in the new model according to the assessment criteria. Following this, the essential components necessary for the new model will be identified from the specific key contributions. These will form the basic structure of the new model. The prevailing models will then be extensively built upon by the construction of a new set of domain-specific components,[10] comprising not only first-layer processes, but also lower-level phases and sub-phases, in order to achieve usability, utility and rigor, as set out by Beebe and Clark (2005). Contribution of the previous models in the form of identified components as well as the new set of constructed components will then be used to develop the new model. The CDFIPM will be graphically represented in the form of UML Activity Diagrams for each given process and its associated lower-level phases and sub-phases. To ensure that the new model is forensically sound, attention will be paid to the criticisms made of the design and implementation of previous models (Adams, 2012). It is intended that the CDFIPM will not only include all the advantages of previous models, but also draw upon the knowledge of a wide variety of experts[11] that cannot be found in the literature.

Activity 4 – Demonstration

After the CDFIPM has been developed, its implementation will need to be demonstrated within an appropriate environment based on the Demonstration Activity of the DSRP. Peffers et al. (2006) suggest the use of case studies as such an appropriate environment. Other researchers in the field (Valjarevic and Venter, 2015; Adams et al, 2014; Casey, 2011; Beebe and Clark, 2005; Ciardhuáin, 2004; Carrier and Spafford, 2003) have also used case studies as an appropriate environment to determine the applicability of their models. Therefore, case studies pertaining to the different fields of law enforcement, commerce and incident response will be used as an appropriate environment for testing the proposed model. The CDFIPM will be applied to the case studies in order to demonstrate its application and effectiveness within the three stated domains. The rationale for selecting different types of case study is to ensure the applicability of the CDFIPM to both forensic and non-forensic investigations. The

[9] Those that have acquired high scores and most closely met the assessment criteria (Adams, 2012).
[10] I.e. those components associated specifically with either law enforcement, commerce or incident response; this approach was originally undertaken by Adams (2012).
[11] These include law enforcement and commercial digital forensic investigators, legal practitioners such as judges and barristers, and experts within academia.

Demonstration Activity will enable any shortcomings to be addressed prior to the submission of the model to independent experts for formal evaluation, which will avoid impinging on the time of the external reviewers. The results of the Demonstration Activity of the research will determine whether the Design and Development stage needs to be repeated in order to make certain alterations.

Activity 5 – Evaluation

Based on the DSRP's requirements, the CDFIPM will be evaluated to determine how well it supports the solution to the stated problem. The evaluations will compare the CDFIPM's application and effectiveness with the characteristics set out in its research aim. During the Evaluation Phase, the CDFIPM will be submitted to digital forensic practitioners within the three domains that are the focus of this research, namely law enforcement, commerce and incident response, and also to judges, barristers and researchers in academia, those being experts within two other domains to which the model has relevance. The aim of such an approach is to enable the author to acquire insightful and reliable feedback as to the effectiveness of the CDFIPM from authoritative external reviewers. As with the Demonstration phase, once the evaluation has been carried out the author will be able to judge whether to repeat the Design and Development Phase of the CDFIPM in order to make improvements. Any such amendments will subsequently be introduced to the design and implementation stages of the CDFIPM.

Activity 6 – Communication

Again, in accordance with the DSRP's requirements, the problem addressed by this research and its importance, its solution (the CDFIPM), its utility and novelty, the rigor of its design and implementation, and its effectiveness will all need to be communicated to the intended user community. The Communication Activity of the DSRP in relation to this research will be achieved through publications in well-known and peer-reviewed journals and conferences. Seven papers will have already been published or accepted for publication within reputable journals and conferences by the time of the thesis submission (see section 6.2 or page iii). The thesis itself will be published within the Research Repository of the University of Derby. In addition, there will be direct

interaction with a wide variety of experts, including digital forensic practitioners, legal practitioners and experts in academia.

1.8 Outline of the Thesis

Chapter 1, Introduction to the Research, explains the background of various issues associated with the existing modes, and concludes by identifying the problem with which this research is concerned. It also presents the research hypothesis, aim, objectives, questions, scope, limitations and assumptions, contribution, and methodology.

Chapter 2, Literature Review, provides a general overview of digital forensic investigations, followed by a detailed review of how the admissibility of digital evidence is governed within the U.K. and U.S. jurisdictions. A critical review is made of the existing models and the different assessment criteria against which previous models will be assessed are introduced. The Chapter then covers the process for identifying those models that can contribute to the design and development of the proposed model by assessing each previous model against the assessment criteria. Following the identification of the prevailing models, their key contributions will be determined based on the assessment criteria. Finally, the components necessary for the proposed model are identified from the key contributions of the prevailing models and all the reviewed models collectively.

Chapter 3, Design and Development, outlines the Design and Development activity for the CDFIPM and provide the rationale behind each stage of the new model.

Chapter 4, Demonstration, covers the process for an initial assessment of the CDFIPM by applying the model to three case studies. This will take place prior to its submission to the external, independent experts for formal evaluation (Adams, 2012, Beebe and Clark, 2005; Carrier and Spafford, 2003).

Chapter 5, Evaluation, details the make-up of the panel of experts, the tasks they will undertake and the results of their evaluation, concluding with a detailed amendment to the CDFIPM (Adams, 2012; Rogers et al., 2006; Ciardhuáin, 2004).

In relation to the research philosophy adopted in this study, since the study requires in-depth and insightful feedback and responses from the study participants, the research, being a qualitative study, draws upon 'Interpretivism' approach to allow the study participants to provide depth and thoughts into their feedback. Therefore, since this research is not looking for a large 'quantity' of data rather the 'quality' of data, the Interpretivism was considered as the appropriate approach in this study.

There are three other main types of research philosophies in addition to the Interpretivism approach, including: Pragmatism, Positivism and Realism. However, since the research philosophy is a vast topic, its detailed discussion is outside the scope of this study. For more information on research philosophies, readers are instead encouraged to refer to Burrell and Morgan's (1985) study that is considered by many researchers (Holden and Lynch, 2004) to be the most comprehensive philosophical framework.

Chapter 6, Conclusion, comprises a detailed conclusion to the research, discussing the research limitations and potential future research opportunities, and includes a detailed summary based on the research aim and objectives. The contribution of the CDFIPM in relation to the field of digital forensics is discussed, as well as how this research has been communicated to date and how it will be communicated in future.

1.9 Summary of the Chapter

This Chapter has provided the rationale for this research, setting out the background and formulating the research problem, its hypothesis, aim, objectives, questions, scope, limitations, assumptions and contributions. The selection of the Design Science Research (DSR) and the Design Science Research Process (DSRP) by Peffers et al. (2006) as the appropriate methodologies to follow during the course of this research has been justified, and the structure of the thesis has been outlined.

Chapter 2: Literature Review

2.1 Introduction

Based upon the Peffers et al's (2006) DSRP – the research methodology used for this research – two resources are required in order to define the "objectives of a solution". These include the "… knowledge of the state of the problem" and "current solutions and their efficacy, if any". The knowledge of the state of the problem for this research was addressed in Chapter 1, where the research problem was defined and the value of its solution justified. This Chapter continues with Peffers et al's (2006) DSRP, gathering further knowledge of the state of the problem and identifying current solutions, if any, and their efficacy. To achieve this, previous models are critically reviewed and assessed in order to identify "prevailing" models which can contribute to the Design and Development of the new model (covered in Chapter 3). This will enable the thesis author to decide upon the necessary components for the proposed model that will constitute the basic structure of the new model's Design and Development.

However, prior to the review and assessment of the previous models, a general review of the topic of Digital Forensic Investigations (DFIs) is provided in section 2.2, followed by a detailed review of the field of digital evidence in section 2.3 and a review of the existing standards associated with the digital investigative process in section 2.4. The discussion of these three topics provides the necessary background for a review and assessment of the existing digital forensic investigation process models (DFIPMs).

2.2 Digital Forensic Investigation

Digital forensics, originally known as computer forensics, first presented itself in the 1970s (Pollitt, 2010). During the first investigations, financial fraud proved to be the most common cause on suspects' computers (Kohn et al, 2013). Since then, digital forensics has grown in importance in situations where digital devices are used in the commission of a crime (Garfinkel, 2010). The original focus of digital forensic investigations was on crimes committed through computers (Casey, 2011). However, over the past few years, the field has extended to include various other digital devices in

which digitally stored information can be processed and used for different types of crimes (Nance et al., 2009). Palmer defines digital forensics as,

> *The use of scientifically derived and proven methods towards 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 unauthorised actions shown to be disruptive to planned operations. (Palmer, 2001)*

This definition is widely accepted within the digital forensic community (Montasari, 2016, a; Valjarevic and Venter, 2015; Kohn et al., 2013; Casey, 2011) and is therefore adopted within this research. A digital forensic investigation (DFI) is the process of linking extracted information and digital evidence in order to establish factual information for review by the judiciary (Casey, 2011; Ioeng, 2006). Cohen (2010) highlights the need to establish factual information as the outcome of such an investigation.

A DFI is carried out as an investigation after the occurrence of an incident (Freiling and Schwittay, 2007; Rowlingson, 2004). It is therefore a distinct type of investigation "where the scientific procedures and techniques used will allow the results, in other words digital evidence, to be admissible in a court of law" (Agarwal et al, 2011). Due to the fact that digital evidence is contained in a digital device and cannot be observed by the naked eye, forensic tools such as Encase (Guidance Software, 2016) and FTK (Access Data, 2016) are used to extract and examine data representing potential digital evidence. The extent of the value of the digital evidence is based not only on the extent to which a tool is trusted (Wojcik et al, 2006; Ciardhuáin, 2004), but also on the competence and experience of the investigator carrying out the digital investigation (ISO/IEC 27037, 2012; ACPO, 2012).

There are four basic principles of DFIs which must be considered. These are auditability, repeatability, reproducibility and justifiability. Auditability refers to the need for an independent investigator to be able to evaluate the activities performed by other investigators to determine whether or not a suitable scientific method was

followed (ISO/IEC 27043, 2015). Repeatability requires one investigator to be able to arrive at the same conclusion as another under similar conditions (Valjarevic and Venter, 2015; von Solms et al., 2006). Reproducibility is established when the same test results are produced using the same method, but with different instruments and under different conditions, and can be reproduced at any time after the original test (ISO/IEC 27037, 2012). Justifiability refers to an investigator being able to justify all the actions and methods they used during the course of a digital investigation (ISO/IEC 27037, 2012).

A DFI is often initiated in order to ascertain certain facts after an incident has occurred. It must be conducted in such a methodical manner that it can withstand scrutiny by the court and defence team (Casey, 2011). There exist various types of DFIs, including live forensics, static forensics, proactive forensics and cloud forensics (Rogers et al, 2006; Beebe and Clark, 2005). The fundamental point of any DFI is to answer 'what', 'why', 'how', 'who', 'where' and 'when' type questions in relation to the data analysis and evidence in order to confirm or refute allegations of suspicious activity (Ioeng, 2006; Kruse and Heiser, 2001). 'What' refers to the data attributes or metadata, 'why,' the motivation (Grobler et al, 2010), 'how,' the manner in which the incident was initiated or the way in which the necessary evidence was isolated (Beebe and Clark, 2005), 'who,' the people involved (Carrier and Spafford, 2003), 'where,' the location of the potential digital evidence (Casey, 2011) and 'when,' the time of occurrence (Mandia et al., 2003).

This research focuses only on the question of "how". Kohn et al. (2013) state that the "how" question is addressed by the steps of the investigative process undertaken which have to be defined. Several authors have defined these steps in a DFPM which is the main subject of this Chapter (review and assessment of the previous models).

2.3 Digital Evidence

2.3.1 Background to Digital Evidence

Nowadays, almost all transactions from the commercial world, government and private individuals exist only in digital form (Cohen, 2012; Casey, 2011; Sommer, 2008). In such cases, it is only through digital evidence that one can demonstrate that something did or did not happen (Kessler, 2010; Rogers et al., 2006). Digital footprints of individuals' activities are left in the digital world, from which their actions and intentions can be deduced (Sommer, 2008). Digital evidence is the product of the digital forensics process (Kessler, 2010; Cohen, 2010 and 2008) and can be extracted from various sources, including digital devices (such as desktop and laptop computers, thumb drives, mobile devices, digital cameras and tablets), network servers (such as supporting applications including Web sites, e-mail and social networks) and network hardware (such as routers) (Casey, 2011; Kessler, 2010; Brown, 2009; Gonzales et al., 2007).

"Forensics" refers to the application of scientific evidence in courts of law, where judges play a vital role as gatekeepers in deciding what evidence is and is not admissible (Kessler, 2010; Cohen, 2010 and 2008; Jones, 2009; Kerr, 2009). Casey (2011) and Palmer (2001) argue that while the actual mechanics of digital forensics are different from the better-known physical and medical forensics, the processes of all forensic sciences are fundamentally the same. Each phase in the process must be performed in such a way that the integrity of the evidence is preserved and its admissibility assured. Digital evidence can be employed in many types of criminal investigations, such as homicide, sex offences, missing persons, child abuse, drugs, fraud and theft of personal information (Casey, 2011). Digital evidence can show how a crime was perpetrated, provide investigative leads, prove or refute witness statements and identify potential suspects. Various similar definitions of digital evidence have been proposed in the literature (Mason, 2007; Rowlingson, 2004; Whitcomb, 2002). However, for the purposes of this research, the following definition given by Casey (2011), which is widely accepted within the digital forensic community, is used:

any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi.

The term "computer" in the above definition can be replaced with "digital device" to cover various types of devices, such as computers, laptop computers, tablets and smart mobile devices. Data in Casey's (2011) definition of digital evidence essentially refers to numbers that represent information of various types such as text, images, audio and video. A simple computer file can contain incriminating information and have corresponding properties that are useful in an investigation. For instance, details such as when a file was created, who may have created it, or that it was created on another computer, can all be essential. Notwithstanding its pervasiveness, few people are well-acquainted with the evidential, technical and legal issues associated with digital evidence.

Consequently, digital evidence is often disregarded, acquired incorrectly or examined and analysed ineffectively. Digital evidence is often challenged in court because of the ease with which it can be altered, which is due to poor handling. The manner in which searches of digital evidence are authorised and carried out, the way in which it is handled, received and rejected, and the various legal issues associated with digital evidence, all differ from one jurisdiction to another. The topic of digital evidence reviewed in this research focuses on the United Kingdom jurisdiction, occasionally incorporating the United States jurisdiction for the purposes of comparison.

2.3.2 Admissibility of Digital Evidence

Digital evidence is increasing in both size and significance in criminal and civil trials (Casey, 2011; Kerr, 2010; Brown, 2009; Kessler, 2010; Cohen, 2010 and 2008; Ball, 2008 and Manes et al., 2007). It is latent in the same way as a fingerprint or DNA sample (ACPO, 2012). However, digital evidence is more complex and volatile as it can be accidently or improperly modified, damaged or destroyed during the investigative process (Giova, 2011; Holder et al., 2009; Mukasey et al., 2008; Bem et al., 2008; Ashcroft et al., 2004). Due to its fragility, courts pay close attention to the process in which the digital evidence was acquired and stored (Kessler, 2010). Investigators'

methods in carrying out digital investigations are often scrutinised by the courts (Montasari et al., 2015; Rogers, 2004). Therefore, to be admissible in court, digital evidence must have all the characteristics of other types of scientific and technical evidence and fulfil the standards associated with them (Casey, 2011; Kessler, 2010). However, electronic-based evidence presents far greater challenges, both for the courts and in relation to the procedures (Kessler, 2010; Sommer, 2008). The manner in which it is extracted plays a significant role in weighing the probative and prejudicial value of the evidence when presented in court (Cohen, 2010 and 2008; Frowen, 2009; Kerr, 2009). To withstand the stringent admissibility requirements, the evidence produced by law enforcement agencies must be robust. Evidence presented in court can be "real", "documentary", "technical", "expert" and "derived" and must satisfy two criteria of "admissibility" and "weight" (Sommer, 2008). To be admissible, it must fulfil legal acceptability tests. This is a function of jurisdiction which derives from English common law rather than European civil codes.

The following three sections discuss the practices carried out by courts in relation to the admissibility of digital evidence. Emphasis is placed on the U.K. courts, but comparisons are also made with the U.S. jurisdiction.

2.3.2.1 Challenges Facing the Judiciary

Judges play a vital role in protecting the legal system from the impacts of flawed evidence (Cohen, 2010). Just as judges need to remove "junk science" from the courtroom, so they need to keep out poor-quality digital evidence (Cohen, 2010 and 2008). They play the role of gatekeeper, determining what evidence is and is not admissible in their courtrooms (Kessler, 2010; Cohen, 2010 and 2008; Jones, 2009; Kerr, 2009). Judges weigh the evidentiary value against the prejudicial effect of any evidence produced (Cohen 2010 and 2008). However, their role has various subtleties and complications. One of the greatest challenges facing both judges and juries (lay audiences) is their lack of proper understanding of digital technology. Kessler (2010) states that for a judge to be able to fairly assess the merits of digital evidence, they need to have some understanding of basic ICTs and the applications from which digital evidence is extracted (Kessler, 2010).

Other researchers have raised this issue, arguing that a lack of familiarity with digital technology and the subsequent detrimental effect on court cases might indicate the necessity for "new laws of evidence" or "specialist judges" (Beebe, 2009; Nance et al., 2009; Shaw, 2006). As there has been no such initiative to date, such a lack of appreciation could prevent judges from critically assessing the evidence submitted to them (Losavio et al., 2006). There is currently no study in the literature in relation to judges' perceived knowledge of digital evidence within the U.K jurisdiction (Kessler, 2010; Scarborough et al., 2009; Rogers et al, 2007; Losavio et al., 2006). This must be considered an imperative subject area for future research.

Technical terms have also proved challenging for judges and juries. For instance, the forensic copy of an evidentiary medium was previously called a "mirror image" (Garber, 2001). Whilst researchers in the field of computer science understand this terminology, it has been misinterpreted by "lay audiences" to denote a reverse copy, as mirrors reflect an opposite image (Brown, 2009; Kessler, 2010). To remove such confusion, the process is now called a bit-by-bit forensic copy (Casey, 2011).

2.3.2.2 United States Jurisdiction

As with any evidence, the proponent of digital evidence has to lay an appropriate foundation in relation to its reliability (Ryan and Shpantzer, 2002). Various practices are carried out across the different jurisdictions in terms of laying such a proper foundation. In the United States, the admission in a federal court of scientific evidence (including digital evidence) is governed by the Federal Rules of Evidence (FRE) (U.S. Courts, 2015; Sommer, 2008). These rules require the trial judge to act as gatekeeper, determining, prior to its admission, whether the evidence is scientifically valid and relevant to the case (Kessler, 2010). Across the U.S. federal courts, judges employ the Daubert Test (*Daubert v. Merrell Dow Pharmaceuticals,* 1993) in order to determine the admissibility of the scientific or technical evidence. The Daubert Test includes the following five assessments:

(1) whether the theory or technique in question can be and has been tested;
(2) whether it has been subjected to peer review and publication;
(3) its known or potential error rate;

(4) the existence and maintenance of standards controlling its operation; and
(5) whether it has attracted widespread acceptance within a relevant scientific community.
(*Daubert v. Merrell Dow Pharmaceuticals,* 1993)

Using the Daubert Test, a judge can objectively determine the reliability of any digital evidence presented in the courts. The *Kumho Tire v. Carmichael* (1999) decision extended the Daubert guidelines to any form of technical evidence. In addition, FRE Rule 702 provides guidelines for qualifying expert witnesses and minimizing adversarial bias in expert testimony (U.S. Courts, 2015). The Rule 702 requirement for reliability may work against its design to balance "the imperatives of maintaining an adversarial system and mitigating bias" (Kessler, 2010). In particular, Rule 702 can be employed to prevent the admission of an expert's assumptions, which a judge might otherwise find useful, as assumptions cannot be considered to be reliable (Bernstein, 2008). In conclusion, the Daubert Test and Rule 702 are employed in the U.S. courts to determine the admissibility of digital evidence as well as any other types of scientific and technical evidence (Kessler, 2010; Rothstein et al., 2007; Meyers and Rogers, 2006; Noblett et al., 2000).

2.3.2.3 United Kingdom Jurisdiction

In the United Kingdom, judges can exercise their discretion within the boundaries of U.K. law (discussed in this section) to dismiss evidence that has been acquired unfairly. In many cases, digital evidence is ruled inadmissible in the U.K. courts if it has not met certain conditions (also discussed in this section). The concept of admissibility requires courts to establish whether evidence is "safe" to place before a jury and whether it will provide a solid foundation for arriving at a decision in the case. In practice, admissibility amounts to a set of legal tests performed by a judge to evaluate an item of evidence (Casey, 2011). This evaluation process can be complex, especially when evidence has not been handled properly or has characteristics that make it less reliable or more prejudicial. In the U.K. legal system, "admissibility" refers to legal rules that are applied to an item of potential evidence prior to a court considering the value of the fact that it claims to offer (Sommer, 2008). There exist various laws and rules that govern the admissibility of digital evidence in U.K. courts.

The most important laws associated with the admissibility of digital evidence are the *Criminal Justice Act 2003,* the *Regulation of Investigatory Powers Act 2000*, the *Computer Misuse Act 1990* and the *Police and Criminal Evidence Act 1984*. For instance, section 117 of the *Criminal Justice Act 2003* regulates the admissibility of communication data that has been obtained under warrant. Under section 17 of the *Regulation of Investigatory Powers Act 2000* content is not admissible. However, it will become admissible if it has been acquired from a foreign law enforcement agency within its own jurisdiction and is available to an investigator to be presented in the U.K. court (Sommer, 2008). Another example is section 78 of the *Police and Criminal Evidence Act 1984*, according to which intercepted data content can only be used for intelligence purposes; it cannot be admitted as evidence. Also, relevant to the issue of the admissibility of digital evidence is whether the material is a "business record," as outlined under section 117 of the *Criminal Justice Act 2003,* an "expert report," defined under section 118(8) and 127 of that Act, or "real evidence". Importantly, under section 78 of the *Police and Criminal Evidence Act 1984,* courts can reject any evidence deemed to have been acquired unfairly.

Compared with the U.K. legal system, admissibility rules in other European counties are much more relaxed and, although admissibility rules in the United States follow the English common law model, they have evolved differently. For instance, authorisations to seize evidence in the U.S. must be drawn up with far greater precision than in the U.K. (Sommer, 2008) and any material acquired outside the warrant is likely to be considered inadmissible. Another deviation relates to the way in which technical evidence is handled. Within the U.K. courts, the jury is simply provided with opposing expert witnesses, while in the United States, technical evidence is an admissibility issue with the judge acting as a gatekeeper to protect the jury from scientific evidence which has not been established as "generally accepted" (*Daubert v. Merrell Dow Pharmaceuticals,* 1993).

U.K. judges often consider three issues before deciding whether or not to admit digital evidence. These can be classified as issues relating to search warrants, reliability and best evidence.

Search Warrants

Acquiring digital evidence under "proper authorisation" is vital for its admission in the U.K. legal system. Investigators must obtain a search warrant or subpoena before they can search, seize or examine digital devices. Subpoenas are employed to seize a company's business records, while search warrants are needed to access more detailed information such as customer-owned files (Casey, 2011). For instance, in circumstances involving an Internet Service Provider (ISP), a subpoena might be required to identify the name of an individual owning a specific e-mail account and a search warrant used to extract the contents of e-mail or user profiles (Kerr, 2009).

As already stated, digital evidence acquired without authorisation will not be admitted in courts. In order to acquire the necessary warrant, investigators must demonstrate to a judge that a crime has been committed, evidence of the crime exists and the evidence is likely to exist at the place to be searched. Search warrants in the United Kingdom can be more loosely defined than in the United States. In the U.K. legal system, there are several types of warrants such as a "specific premises warrants", all-premises warrants" and "multiple entry warrants" (Casey, 2011). Even when investigators have obtained authorisation to search a computer, they must focus only on the crime under investigation. If they identify evidence of other crimes during their investigation, that evidence will not be admissible as it is outside the scope of the warrant. In such circumstances, investigators would have to obtain a second warrant before being able to use evidence to charge the offender (Casey, 2011; Sommer, 2008).

Furthermore, investigators may need to acquire two separate warrants for a seized computer: one for the computer itself and one for the files contained in it. Seized computers usually constitute "real" evidence for admissibility purposes, with individual files having to be admitted separately in accordance with section 117 of *Criminal Justice Act 2003*. This is of particular importance where more than one individual has had access to a computer. In such situations, in order to adhere to *Computer Misuse Act 1990*, investigators must prove that they are authorised to access the computers.

Reliability

In the U.K. courts, digital evidence is also considered for its "weight of fact", "persuasiveness" or "probative value" (Sommer, 2008). Since digital evidence is not considered different from text contained within a document, it is subject to the same rules and laws as documentary evidence. Therefore, the responsibility lies with the prosecution to prove that the evidence is no more or less at the date of the court hearing than it was when it was taken into the possession of police (ACPO, 2012). This is why it is so important for investigators to demonstrate that digital evidence is reliable, otherwise it will not be admissible. Certain conditions must be fulfilled before digital evidence will be considered reliable, and they are often the same across the U.K. and U.S. jurisdictions (Adams, 2012; Steel, 2006). To be considered reliable, digital evidence must be "authentic", "accurate" and "complete".

To demonstrate its authenticity, investigators must be able to specifically link the digital evidence to the alleged crimes and individuals in the case (Casey, 2011; Kessler, 2010; Sommer, 2008). They must also prove that the recovered evidence is the same as originally seized data, demonstrating that the evidence was extracted from a particular computer or location and that a "complete" and "accurate" copy was acquired. They must be able to prove how the evidence was acquired by demonstrating each process through which it was collected. This is not only to demonstrate that evidence has not been modified during the processing, but also to prove that no mistakes have been made by the investigators or the tools employed (Sommer, 2008).

Investigators will need to make a forensically sound copy[12] [13] of the medium containing potential digital evidence (Montasari, 2016, c; Brown, 2009) and conduct the examination and analysis on the "working copy". This is to protect the integrity of the original data and to ensure that the original evidence is not contaminated (Montasari, in press, b; Casey, 2011; Kessler, 2010). Therefore, they will need to demonstrate that an authentic copy of the original data was created (ACPO, 2012; Brown, 2009; Casey, 2011). To prove that there has been no contamination or modification, investigators

[12] The imaging process often duplicates the original evidence in fixed-size blocks to the "examination medium" and each block is individually validated (Kessler, 2010).
[13] In certain circumstances, partial or selective imaging might also be regarded as acceptable, for instance in cases where the storage size is very large, and it is not practicable to image a large volume of data.

need to show that the evidence has been subjected to digital fingerprinting and the original digital fingerprint matches the presented exhibit (Montasari, in press, b; Kessler, 2010; Sommer, 2008). The most commonly employed algorithms for verifying data in digital forensics are MD5 and SHA-1 (Casey, 2011). Investigators must also demonstrate that the imaging process can be reproduced, in order that two different qualified practitioners can create identical forensic replicas by employing the same hardware and software when considering the same original (Casey, 2011; Brown, 2009).

As stated above, to meet the requirement of reliability, investigators need to demonstrate that digital evidence has remained unchanged since it was acquired. The "Chain of Custody" plays a vital role in proving the authenticity of digital evidence. This refers to the necessity to maintain detailed notes and to report every action performed on an item of evidence, from the moment it was collected to the point that it is presented as an exhibit. Such notes must detail the sources of the data, record which proven tools and techniques were employed and demonstrate that the data has not been modified since it was extracted through maintaining hash values such as MD5 and SHA-1 (Montasari, 2016, c; Casey, 2011). A proper chain of custody will prove that digital evidence was extracted from a particular system or location and has been continuously controlled since its acquisition.

Proper chain of custody documentation allows the court to relate the digital evidence to the crime. Inappropriate documentation may lead to confusion over how and where the digital evidence was acquired, raising doubts about its reliability. In terms of the evidence itself, although it is often a computer hard-disk or other type of digital device that is seized, what actually needs to be placed before the court is often a number of accurate "printouts" or "screen dumps" [14]. Therefore, it is also important for investigators to demonstrate that the printout is complete and reliable, and who produced it. As stated above, a whole computer or other item of data storage media is admissible as "real evidence," with items derived from it following digital examination and analysis being separate exhibits in their own right, such as printouts and screen

[14] UK courts are often uncomfortable with the idea that the whole computer system is presented to them.

captures. These separate exhibits become admissible if the investigator who conducted the extraction can attend court to produce the exhibit and be cross-examined.

In terms of proving the accuracy of digital evidence in courts, some researchers (Buskirk and Liu, 2006), as also cited by Adams (2012), argue that if it is accepted and admitted in court, it is both reliable and correct. This argument is flawed as inconsistencies in forensics software, errors in the imaging process and differences in practitioners' knowledge can negatively impact upon the reliability, accuracy and integrity of digital evidence. This is supported by Kessler (2010), Cohen (2010 and 2008) and Casey (2002). Therefore, digital evidence must be free from any reasonable doubt concerning the quality of procedures employed to acquire the material, examine it and present it to the court. The evidence must be produced by an individual (often a digital forensic analyst) who can describe the processes followed to produce the evidence. Digital forensic methods employed to acquire and process the evidence must be clear, such that it can be tested by third-party experts. In circumstances where exhibits themselves include statements, the requirement for accuracy extends to the content. Investigators producing documents provide a witness statement and must be available for cross-examination in court. Finally, the term "completeness" refers to the requirement for a complete history of the specific set of circumstances or events.

Best Evidence

The "best evidence" rule refers to a legal principle that an original copy of a document is superior evidence. In the past, based upon this rule, secondary evidence such as a copy or "facsimile" would not be admissible if an original document was in existence and could be acquired (Ormerod and Perry, 2015). The original purpose of the rule was to ensure that decisions reached in courts were based on the best available information (Casey, 2011). However, with the arrival of photocopiers, scanners, computers and other technology that can produce effectively identical replicas, duplicates became acceptable instead of the original. According to Blackstone's Criminal Practice 2014 (Ormerod and Perry, 2015), the best evidence rule in England and Wales is now all but defunct. Therefore, evidence that is not an original will be admitted provided it meets other admissibility requirements. If a question is raised in relation to the authenticity of the original or the accuracy of the copy, or if the circumstances dictate that it would be

unfair to admit the copy in place of the original, the best evidence rule will still apply. As most forms of digital evidence can be duplicated exactly, this issue does not often arise and copies are usually admitted in the U.K. courts. In fact, producing a duplicate of digital evidence is often preferred as it removes the possibility of the original being accidently modified. According to the "Hearsay Rule"[15], digital evidence would not be admissible if the witness (the digital forensic analyst) was not present in court to verify its truthfulness.[16]

2.4 Standards and Guidelines

Since Digital Forensic Science is a new discipline, there is a limited number of standards and guidelines related to the field. Those standards in existence, however, do not cover jurisdiction-specific requirements that relate to issues such as admissibility, evidential weighting, relevance and other judicially controlled limitations on the use of potential digital evidence in courts of law. This view is supported by the UK Forensic Science Regulator, who states,

> *Standards such as ISO/IEC27037:2012 may be used as guidance if required, however they are not equivalent and cannot be used as a substitute for the accreditation standard.* (Forensic Science Regulator, 2016)

Furthermore, these standards and guidelines are not generic as each has a specific focus on a particular field such as law enforcement, electronic discovery, commercial digital forensics or incident response. The existing standards and guidelines usually capture only parts of the investigative process as opposed to covering the entire process. The key standards and guidelines identified through the process of literature review are discussed in this section.

[15] Under section 114(1) of the *Criminal Justice Act 2003*, "hearsay" in criminal proceedings is "a statement not made in oral evidence in the proceedings that is evidence of any matter stated."
[16] There are exceptions for evidence that describes events accurately and is simpler to authenticate, but the discussion of these is outside the scope of this research.

2.4.1 ISO/IEC 27035:2011

ISO/IEC 27035 (2011) is an international standard that provides guidance only on "information security incident management" for organizations. This standard is not comprehensive as it only covers guidelines in relation to incident detection and first response. It consists of two parts contained in two separate documents. Part one provides guidelines on detecting, reporting, assessing and managing information security incidents, while part two provides guidelines on planning and preparing for incident response. This standard is only aimed at corporate investigation, and excludes other fields such as law enforcement.

2.4.2 ISO/IEC 27037:2012

The ISO/IEC 27037 (2012) is an international standard developed by the Joint Technical Committee of ISO (the International Organisation for Standardisation) and IEC (the International Electrotechnical Commission), providing guidelines for activities in dealing with potential digital evidence. This standard only deals with the initial digital evidence handling process including: Identification, Collection, Acquisition and Preservation (the post-mortem[17] stages). No pro-active activities are incorporated into ISO/IEC 27037, such as Forensic Readiness Process (Montasari, 2016, c; Valjarevic and Venter, 2015; Rowlingson, 2004; Mandia et al., 2003) which is essential for advanced planning and preparation prior to incident detection. Other important processes that this standard lacks include: Examination, Analysis, Presentation and Investigation Closure.

Furthermore, ISO/IEC 27037 (2012) does not address activities associated with legal proceedings in handling potential digital evidence. Since it is an "international" standard, it does not cover jurisdiction-specific requirements that relate to issues such as admissibility, evidential weighting, relevance and other judicially controlled limitations on the use of potential digital evidence in courts of law. Since ISO/IEC 27037 cannot replace specific legal requirements of any jurisdiction (nor any other standards), investigators would need to adapt it so that it could comply with the "national" laws,

[17] Post-mortem processes are the reactive measures utilised to investigate an incident after it has taken place.

rules and regulations. The main advantage of this standard is that it has provided some level of details in relation to its data acquisition process, which the new model will draw upon. However, this standard is incomplete on its own and should be used in conjunction with other standards concerning digital evidence and the investigation of information security incidents.

2.4.3 ISO/IEC 27043:2015

ISO/IEC 27043 (2015) describes processes relevant to different kinds of investigations, such as unauthorized access and corporate breaches of information security. Authors of this standard claim that it is comprehensive since it is based on the harmonisation of fourteen of the previously proposed DFIPMs. Although ISO/IEC 27043 has attempted to capture the entire investigative process, the Processes included in this standard are overly high-level without any lower-level details, i.e. Phases and Sub-Phases, to assist the investigators. Beebe and Clark (2005) supported by Montasari (2016, c) and Kohn et al. (2006) criticise such an approach arguing that the complexities of the digital investigative process cannot be represented at such a high level.

To elaborate their points further, they draw a useful analogy stating that supposedly flying an airplane were a function of a higher order framework consisting of three Phases: "take-off", "fly" and "land", very few pilots could achieve this task without acquiring further details in relation to each of the Phases. Similarly, greater detail associated with each stage of a digital investigative process is required in order to enhance the usability of the forensic methodology for DFIs. This is, however, is missing in ISO/IEC 27043 (2015). Authors of this standard, themselves, admit such a shortcoming stating,

> *This International Standard provides a general overview without prescribing particular details within each of processes covered in this International Standard ISO/IEC 27043 (2015).*

ISO/IEC 27043 has not also provided any details in relation to the activities associated with live acquisition of the potential digital evidence, nor has it specified certain important processes such as evaluating and securing the crime scene. As ISO/IEC

27043 documentation itself states, this standard will need to be used in conjunction with other international standards including: ISO/IEC 27035, ISO/IEC 27037, ISO/IEC 27042 and ISO/IEC 27041.

2.4.4 British Standards Institute (BSI)

British Standards Institute developed BS 10008 Standard (BS 10008, 2014) , which outlines the requirements for:

- addressing issues associated with the authenticity and integrity of the electronic information;
- transferring information from one computer system to another electronically; and
- implementing and operation of electronic information management system.

The BS 10008 also outlines the requirements for the management of the availability of electronic information and addresses issues in relation to:

- electronic copyright systems;
- electronic identity verification;
- linking of electronic identity to particular electronic documents; and
- use of electronic signatures.

Although the requirements outlined in BS 10008 are generic, this standard only applies to corporate environment, and excludes other domains such as law enforcement.

2.4.5 Association of Chief Police Officers (ACPO)

In the United Kingdom, the National High-Tech Crime Unit has produced the Good Practice Guide for Digital Evidence on behalf of the Association of Chief Police Officers with its main focus being on the field of law enforcement. This guide has been updated several times with the latest one being Version 5 in October 2011 (as of May 2016). In the latest version of this guide, the 'computer-based evidence' was replaced

with ‘digital-based evidence’ to reflect the development of investigating cyber security incidents in a broader context. This guideline consists of four principles as follows:

> Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
>
> Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
>
> Principle 3: An audit trail or other record of all Processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Since ACPO Good Practice Guide does not form a legal requirement within the UK jurisdiction, its application by DFIs is voluntary.

2.4.6 Other Guidelines

Other guidelines with a single author have been reviewed and assessed under the “Model Assessment” section in this chapter. These include guidelines by the US Department of Justice (Ashcroft, 2001) and the National Institute of Standards and Technology (Kent et al, 2006).

2.5 Method of Identifying the Previous Models

In order to perform a successful literature review, various online data resources accessed via the library of University of Derby were utilised. The online data resources included, but were not limited to, Science Direct, IEEE and ACM digital libraries. Journal articles and conference proceedings related to this research were identified and

downloaded for study through the three aforementioned digital libraries. Moreover, online search engines in particular Google Scholar, university repositories, governmental and reputable websites were used to identify papers related to this research. Other resources of data included books and special magazines. In order to identify the relevant papers, various search terms were performed, either unaccompanied or in combination. These included: Computer forensics, digital forensics, process model, framework, methodology, ad-hoc, standards, collection, examination, guidelines, incident response, cybercrime, imaging and digital evidence. To ensure that all the papers containing the previously developed process models have been identified, the references in already-identified papers were cross-checked to ensure that no relevant paper was missing (an approach also taken by Adams (2012)).

2.6 Assessment Criteria for the Previous Models

Following on from the research aim, the underlying requirements of a digital forensic investigation process model are that:

- The model must be comprehensive and detailed in that it encompasses the entire investigative process and contains granularity (low-level details).

- The model must be formal in that it harmonizes and integrates previous models by creating a synergy between different points of view and then builds upon the models extensively.

- The model must be generic in that it can be applied to both law enforcement and corporate investigations.

As well as taking into consideration the research aim when assessing the previous models, three further different sets of assessment criteria have been employed to determine those models that can contribute to the design and development of the new model. This is to establish whether there are any aspects of those "prevailing" models that can be used to assist in the design and development of the CDFIPM. The three sets of assessment criteria that have been used as a framework against which the previous

models will be judged include: (1) the four-point requirement suggested by Beebe and Clark (2005), (2) the five-point requirement proposed by Carrier and Spafford (2003) and the five-point requirement set by Daubert Test (*Daubert v. Merrell Dow Pharmaceuticals,* 1993).

To assess each previous model against the three sets of assessment criteria, each model will be given three different scores, each of which refers to a particular set of criteria. The score given to each model in relation to a particular set of criteria will be based on how many of the requirements in that particular criteria have been met. The score-based approach used to assess the previous models is adopted on the basis that there are no other studies from which assessment data for previous models could be extracted (Adams, 2012). Although two other researchers (Adams, 2012; Beebe and Clark, 2005) have used evaluation criteria for assessing previous models, their approach has been limited either to two sets of assessment criteria (Adams, 2012) or to one set of assessment criteria (Beebe and Clark, 2005), namely those of the Daubert Test (*Daubert v. Merrell Dow Pharmaceuticals,* 1993) and Carrier and Spafford (2003).

Thus, assessing the previous DFIPMs against "three" different assessment criteria have been conducted for the first time in the field of digital forensic science, which is another novel contribution of this research. Such an approach should not, however, be considered as a conclusive assessment. Instead, the score-based assessment employed is used to score the previous models in order to determine (as closely as possible) how many of the requirements of each given criteria have been fulfilled by a given model (Adams, 2012).

2.6.1 Beebe and Clark's Four-Point Requirement

The followings summarize the four-point requirement set by Beebe and Clark (2005) against which the previous models can further be judged:

1. A model must achieve scientific rigor and relevance.
2. A model must simplify complex process to facilitate understanding of the underlying structure.

3. A model must retain enough granularity[18], or the flexibility to incorporate granularity needed to exploit the framework in unique situations.
4. A model must delineate standard assumptions, concepts, value and practices.

The above four requirements can be explained in further detail:
Rigor is attained through the use of Classes[19] and Processes approach and the inclusion of important Principles, and the relevance is achieved via the use of objectives-based Phases and Sub-Phases. In other words, in order for a model to achieve both rigor and relevance, it must be comprehensive such that it contains not only the higher-order layers, i.e. 'Classes', 'Processes', but also lower-level components, i.e. 'Phases' and 'Sub-Phases', as well as important 'Overriding Principles' such as maintaining detailed documentation or preserving a chain of custody (requirement 1). Simplification of complex digital investigative process can be achieved through a hierarchical process model which allows its users to focus on higher order layers abstractly (requirement 2). At the same time, granularity is achieved by incorporating multiple layers of details into the model, i.e. Processes, Phases and Sub-Phases (requirement 3). Finally, a model can delineate standard assumptions, concepts, values, and practices through the use of constraints, definitions, principles, objectives, and task hierarchies.

To judge each previous model against Beebe and Clark's (2005) assessment criteria, each model will be given a score out of "4" on the basis of how many of the four requirements have been met. To the thesis author's best knowledge, no other researcher in the literature has used Beebe and Clark's (2005) four-point assessment criteria previously to assess either their own models or the models proposed previously. Thus, this four-point requirement has been used for the first time to assess the existing models in this thesis.

[18] In this context, granularity refers to the extent to which a model is broken down into lower-level details (behavioral entities). Granularity is also the level of detail considered in a model or decision making process. The greater the granularity, the deeper the level of detail. Granularity is usually used to characterize the scale or level of detail in a set of data.
[19] In the context of this study, the term 'Class' does not refer to the same term employed in object-oriented programming, in which a class is a template definition of methods and variables in a particular. Instead, the word 'Class' is used throughout this study simply to refer to the specific category in which the proposed model's Processes are placed.

2.6.2 Carrier and Spafford Five-Point Requirement

Carrier and Spafford's (2003) five-point requirement set[20] by which the previous models can be further assessed are summarized as follows:

1. The model must be based on existing theory for physical crime investigations;
2. The model must have practicality matching steps taken in actual investigations;
3. The model must be technologically neutral to ensure that the process isn't constrained by current products and procedures;
4. The model must be specific enough that general technology requirements for each phase can be developed;
5. The model must be abstract and apply to law enforcement investigations, corporate investigations and incident response.

As with Beebe and Clark's (2005) assessment criteria, to assess each previous model against Carrier and Spafford's (2003) five-point requirement, each model will be given a score out of "5" on the basis of how many of the five requirements have been accomplished.

2.6.3 Daubert Test Five-Point Requirement

The third set of assessment criteria that have been used to assess the previous models is that as outlined in the Daubert Test (*Daubert v. Merrell Dow Pharmaceuticals,* 1993)[21]. This test has also been selected based on the fact that it is a set of commonly-referenced criteria to judge the reliability of scientific evidence by many courts (Valjarevic and Venter, 2015; Casey, 2011). The Daubert Test is used in many federal as well as some state courts in the United States to make an initial assessment of whether an expert's scientific testimony is based on reasoning or methodology which is scientifically valid and can properly be applied to the facts (Cornell University Law School, 2016). Using this test, the criteria that must be taken into consideration in establishing whether the methodology is valid include a set of "5" requirements as outlined in the section 2.3.2.2.

[20] Carrier and Spafford's (2003) five-point requirement have also been used by Beebe and Clark (2005) to assess their own model against as well as by Adams (2012) to assess the previous DFIPMs against.
[21] The Daubert Test has also been used by Adams (2012) for the first time in the field of digital forensics to assess the previous models against.

Similar to Beebe and Clark's (2005) and Carrier and Spafford's (2003) assessment criteria, to assess each previous model against Daubert Test five-point requirement, each model will be given a score out of "5" on the basis of how many of the five requirements have been achieved.

2.7 Review and Assessment of the Previous Models

2.7.1 Palmer's FDFS

On August 2001, the first Digital Forensic Research Workshop took place in Utica, New York. This gathering was held in order to stimulate discussion among academics and practitioners with experience and interest in the field of Digital Forensic Science. The purpose of this workshop was to initiate establishing a community of interested individuals for defining the domain of digital forensics and identifying the difficult challenges facing the field. The conference also included a session entitled "A Framework for Digital Forensic Science (FDFS)", the aim of which was to "build a taxonomy to guide and direct research" and "identify the areas or categories that define the universe of Digital Forensic Science" (Palmer, 2001).

The first effort to categorise digital forensic investigative process was made in the DFRWS's final paper (Palmer, 2001) and included seven processes that were extracted from steps employed in digital forensic analysis. The seven Processes included: Identification, Preservation, Collection, Examination, Analysis, Preservation and Decision as represented in Figure 2. However, out of the seven Processes, the attendees identified only four processes, namely Preservation, Collection, Examination and Analysis, as core Processes even though many other researchers would dispute the forensic nature of each step of the process (Kohn et al, 2013; Casey, 2011; Pollit, 2009). Finding the consensus on exactly what comprises the "forensic process" appears to have been challenging with the final summary defining the incorporated Processes as being "…subject to the least confusion" amongst researchers and practitioners (Palmer, 2001).

Content was removed for copyright reasons.

Palmer, G. (2001). 'A Road Map for Digital Forensic Research', *First Digital Forensic Research Workshop (DFRWS)*, pp. 27-30.

Figure 2. The FDFS after Palmer (2001)

Although the Framework for Digital Forensic Science (FDFS) is a valuable source as a starting point, it was never intended to be the final model but instead as a foundation for future work that would define a full model and also as a framework for future research. The FDFS has come under criticisms by other researchers. Reith et al. (2002) has criticised the model for being incomplete, while Baryamureeba and Tushabe (2004) have taken an issue with the model for its lack of descriptions for each given Process. Similarly, Ciardhuáin (2004) has criticised the model for the fact that it "does not discuss the steps of the model" and the fact that the model has a linear representation. Adams (2012) is also critical of this model for repetitions, stating "… preservation appears four times under different categories".

There are various other shortcomings associated with the FDFS. The model is missing some very important investigative process such as Forensic Readiness, First Response, Secure and Evaluate the Crime Scene, Interpretation, Event Reconstruction, Reporting and Presentation. The model has not also accommodated steps for digital evidence management such as those activities related to return, destruction or cleansing and

reusing of digital evidence. More importantly, the FDFS has not incorporated the investigative principles which need to be carried out throughout the entire investigative process for the purposes of conducting forensically sound investigations. The missing Principles include those pertaining to 'Maintaining a Detailed Documentation', 'Preserving Chain of Custody', 'Maintaining Information Flow', 'Interacting with Physical Investigation', 'Obtaining and Adhering to the Proper Legal Authorisation' and 'Addressing Safety Issues'. It is reasonable to attribute the aforementioned stated criticisms and shortcomings to the fact that this model was the first attempt to define the digital investigative process. In fact, the group (Palmer, 2001) themselves admitted that the model would need to be further developed in the future stating, "… Of particular interest is the need for continued development of methodologies employed within the discipline."

In terms of the Beebe and Clark criteria the FDFS meets only Requirements 2 and 3 as it is simple enough to be employed and also allows for the model to be infused with further details. However, the model does not have scientific rigor or relevance due to its missing investigative processes as well as its lack of lower level details (Requirement 1). The FDFS has not also been capable of properly defining its concepts, such as those associated with the investigative principles (Requirement 4). The Beebe and Clark score given to this model is 2/4.

In relation to the Carrier and Spafford criteria, the FDFS meets only Requirements 3 and 4 as it is not dependent on a particular technology (Requirement 3), and it is also specific enough to allow for the technology to be used to help the investigators (Requirement 4). However, the model has no basis in theory for physical crime scene investigation (Requirement 1), nor is it practical since it has omitted some essential stages of the investigative process (Requirement 2). Moreover, the model is not generic as it is only applicable to the field of law enforcement (Requirement 5). The Carrier and Spafford score given to this model is 2/5.

Based on the Daubert Test, the FDFS only meets Requirements 2 as it has been peer-reviewed and published. However, there is no evidence suggesting that the model has been tested (Requirement 1); as a result, its potential error rate is unknown (Requirement 3). There is also no evidence showing that the model has referenced or

drawn upon any standard (Requirement 4). This might be explained by the fact that at the time there were no proper guidelines associated with the field of digital forensic science. Moreover, although the subsequent DFIPMs were developed as a result of the FDFS, there is no evidence suggesting that the model has been widely accepted within the field of digital forensic community. The Daubert Test score given to this model is 1/5.

2.7.2 US Department of Justice's ECSIGFR

The U.S. Department of Justice published a process model in the "Electronic Crime Scene Investigation: A Guide for First Responders" (Ashcroft, 2001), that consists of the following phases: Preparation, Collection, Secure and Evaluate the Scene, Document the Scene, Evidence Collection, Examination, Analysis and Reporting. This guide is a first responder's reference to various types of electronic evidence and consists of procedures that can be employed to handle them safely. The ECSIGFR is aimed at the investigators who respond to the physical crime scene; therefore, its focus is on those requirements. This process model has only focused on the middle part of the investigative process missing important stages such as those related to the case initialisation and those associated with the investigation closure. The ECSIGFR is also missing the "Presentation" Process, where the results of the investigation should be presented to the relevant audience.

The ECSIGFR is very ambiguous in terms of the descriptions attached to its components. For example, it regards the collection of the "physical hard disk" to be the collection of "electronic evidence". However, at this point in any digital investigation, it is very normal for investigators not to know whether the physical hard disk contains pertinent electronic evidence or not. In line with the view of Montasari et al, (2015), Valjarevic and Venter (2015), Rogers et al. (2006) and Carrier and Spafford (2003), the collection of evidence very often takes place after it has been identified. However, in this model, the evidence is collected before the digital data has been examined. In their paper, Carrier and Spafford (2003) also highlight this issue, stating that the Collection Phase more precisely should collect the physical evidence, and the individual pieces of electronic evidence must be collected when it is examined.

Since the ECSIGFR's components have been improperly defined, their objectives have also been confused. For instance, the model has confused the "Analysis" Process with the "Interpretation" Process even though these two must be treated as two different Processes (Analysis must be carried out first so that its results can be interpreted next). This is due to the fact that both processes have different objectives, and each of them requires a unique set of investigative techniques to be performed properly.

In relation to the Beebe and Clark four-point requirement, the ECSIGFR has only met Requirement 2 as it allows its users to focus on higher order layers abstractly. However, the model has no scientific rigor or relevance as it is not detailed and is missing essential stages of the investigative process (Requirement 1). The model does not also have sufficient granularity, or does not allow for new layers of details to be added to it (Requirement 3). The model's components are also improperly defined (Requirement 4). The Beebe and Clark score given to this model is 1/4.

With regards to the Carrier and Spafford criteria, the model only meets Requirements 1 and 3, as it has basis in existing theory for physical crime scene (Requirement 1), and it is not dependent on a particular technology (Requirement 3). However, the ECSIGFR is not practical as it misses many steps that are parts of the actual investigative process (Requirement 2). Also, the lack of guidance in its application and also ambiguous descriptions have prevented the design of technological tools to aid DFIs (Requirement 4). Moreover, the model is not applicable to various user communities as its only focus is on the field of incident response (Requirement 5). The Carrier and Spafford score given to this model is 2/5.

Concerning the Daubert Test, the ECSIGFR has not met any of the requirements. There is no evidence suggesting that the model has been tested (Requirement 1); thus, its potential error rate is not known (Requirement 3). The model has also not been subjected to peer review and publication (Requirement 2). Moreover, there is no evidence suggesting that the model is based on a particular standard (Requirement 4), nor is there any evidence demonstrating that the model has been widely accepted in the digital forensics community (Requirement 5). The Dauber Test score given to this model is 0/5.

2.7.3 Reith et al's ADFM

Criticizing the previous methods for being too technology specific, Reith et al. (2002) proposed the ADFM in an attempt to improve upon the previous models via "the amalgamation of common techniques" while attempting to ensure method shortfalls were addressed. Reith et al. (2002) identified the common components from the previous models and incorporated those common components into their Abstract Digital Forensic Model. Although the ADFM is mainly based upon the initial model of Palmer (2001), it adds a description for each Phase. This model is based on nine phases as follows:

- Phase 1 (Identification) is where an incident is detected, and its type is determined.
- Phase 2 (Preparation) involves preparing tools, techniques, authorisations and management support.
- Phase 3 (Approach Strategy) includes developing an approach based on the potential impact on bystanders and the specific technology in question.
- Phase 4 (Preservation) involves preserving the state of physical and digital evidence by preventing people from using the device containing potential digital evidence or using any electromagnetic device within an affected radius.
- Phase 5 (Collection) includes recording the physical scene and duplicating digital evidence using standardized and accepted procedures.
- Phase 6 (Examination) involves the investigators performing an in-depth search of evidence concerning the suspected crime.
- Phase 7 (Analysis) requires the investigators to determine significance, reconstruct fragments of data and draw conclusion based on the evidence found.
- Phase 8 (Presentation) involves summarising the conclusions that should be provided in a layperson's terms using abstracted terminology.
- Phase 9 (Return Evidence) involves returning physical and digital evidence to its rightful owner.

Unlike many other process models where Examination and Analysis are treated as a single phase, Reith et al. distinguishes between the two processes. Examination Phase in this model involves investigators performing an in-depth search of evidence concerning

the suspected crime, while the Analysis Phase requires the investigators to determine significance, reconstruct fragments of data and draw conclusion based on evidence found. However, Carrier and Spafford (2003) have criticised such an approach arguing that that the names of the Examination and Analysis Phases included in this model can be confusing because their meaning is only slightly different, and it is common to have two investigators who are referring to the same tasks when they say that they are "analyzing a system" or "examining a system". This criticism seems to be invalid as the Examination and Analysis have different aims and therefore should be assigned two separate phases. Examination Phase should involve activities regarding the extraction of potential digital evidence from the acquired data (Montasari, 2016, a and c; Kohn et al., 2013), whereas the Analysis Phase should involve activities related to the methodical analysis of the digital evidence as well as the construction of the incident (Montasari, 2016, a and c; Casey, 2011). Although this model provides a general framework that can be applied to a range of incidents, it has various shortcomings, some of which are identified by the authors themselves. Reith et al. (2002) acknowledge three disadvantages of applying their model as follows:

- Categories may be defined as too general for practical use
- There is no easy or obvious method to test the model.
- Each sub-category added to the model will make it more cumbersome to use. In other words, as the model is expanded to increase its granularity, it becomes more complex and more cumbersome to use (Adams, 2012).
  (Reith et al, 2002)

In addition, although 'Chain of Custody' is a vital aspect of any digital forensic investigation, this investigative Principle has not been explicitly incorporated into the ADFM, a point also raised by Adams (2012) and Ciardhuáin (2004). Instead, Reith et al. (2002) have stated, "This model assumes that a strong chain of custody will be maintained throughout the duration of the investigation. The absence of it on the model above makes no presumptions that it is not important, only that it is implied in any discussion of forensics." Ciardhuáin (2004) criticizes the Reith et al's (2002) model for its lack of explicit mentioning of the "Chain of Custody" stating,

The single largest gap in the existing models is that they do not explicitly identify the information flows in investigations. For example, Reith et al. (2002) themselves have noted the absence of any explicit mention of the chain of custody in their model. This is a major flaw when one considers the different laws, practices, languages, and so on which must be correctly dealt with in real investigations.

Other authors such as Boddington t al. (2008), Peisert et al. (2008), Selamat et al. (2008), as cited by Adams (2012), adopt the same criticism of the AFPM for its lack of the explicit inclusion of the "Chain of Custody". However, in accordance with the ACPO Good Practice Guide for Digital Evidence (2012), ISO/IEC 27043 (2015) and other researchers including Montasari (2016, c), Valjarevic and Venter (2015), this important investigative Principle must be explicitly covered in a DFIPM. Further shortcomings of the ADFM relates to some important stages of digital investigation that are absent in this model. For instance, the model does not contain a Forensic Readiness stage as emphasised by Montasari et al. (2015), by ISO/IEC 27043 (2015), ISO/IEC 27035 (2012) and Rowlingson (2004) to ensure that both Infrastructure Readiness and Operational Readiness are in place prior to a possible incident or security breach. One might argue that the Preparation Phase of the ADFM would simply accommodate for the Forensic Readiness activities. However, the Preparation Phase included in this model is mainly focused on the activities related to a law enforcement environment. Also, a distinction always needs to be made between the Forensic Readiness Phase referring to the readiness of the organisation as a whole and the Preparation Phase referring to the readiness of the investigators, a view implicitly supported by Valjarevic and Venter (2015), Kohn et al. (2013), Rowlingson (2004) and Carrier and Spafford (2003). Another major drawback of this model is associated with its lack of graphical representation.

In relation to the Beebe and Clark criteria, the ADFM meets Requirement 4 fully and also meets Requirements 1 and 3 partially. The model is clear in the description of its Phases even though it lacks investigative principles (Requirement 4). The ADFM has also achieved scientific rigor and relevance to some extent as it has captured most of the investigative stages despite missing some steps (Requirement 1). Furthermore, although the model has not incorporated lower-layers of details, it allows for the model

to be infused with additional details (Requirement 3). However, the ADFM has not been capable of simplifying the complex investigative process as the model lacks graphical representation (Requirement 2). The Beebe and Clark score given to this model is 2/4 as the model meets Requirements 1 and 3 partially.

In terms of the Carrier and Spafford criteria, the ADFM meets all the requirements except Requirement 2. The model has a basis in existing physical crime scene theory (Requirement 1), and it is not dependent on a specific technology (Requirement 3). The ADFM is also specific enough to allow for technology to be developed to assist the investigators. Moreover, the model is relevant to both law enforcement and corporate investigations (Requirement 5). However, the model has major drawbacks in relation to practicality and its capability to accommodate changes without becoming overly complicated (Requirement 2). The Carrier and Spafford score given to this model is 4/5.

Based on the Daubert Test, the ADFM meets only Requirement 2 as the model has been subjected to peer review and publication. However, as Reith et al. (2002) themselves admit, the ADFM has not been tested (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). There is also no evidence suggesting that the model is based on a standard (Requirement 4), nor does there exist evidence of the model having been widely accepted within the digital forensic community (Requirement 5). The Daubert Test score given to the AFPM is 1/5.

2.7.4 Carrier and Spafford's IDIP

The Integrated Digital Investigative Process (IDIP) developed by Carrier and Spafford (2003) has seventeen Phases organized into five groups as illustrated in Figure 3. This model applies physical crime scene Processes into the digital crime scene with the computer being treated as a "door to another room". In order to describe the differences and similarities between a physical and digital crime scene, Carrier and Spafford define the physical crime scene as "an environment where physical evidence of a crime or incident exists". The environment where the first criminal act occurred is the primary physical crime scene and subsequent scenes are secondary physical crime scenes. The

digital crime scene is also defined as "the virtual environment created by software and hardware where digital evidence of a crime or incident exists".

Although Carrier and Spafford's IDIP is considered to be one of the most prominent process models presented to date (Montasari 2016, a, b and c, Valjarevic and Venter 2015; Adams, 2012, Beebe and Clark, 2005), it is open to some valid criticisms. For instance, the model represents the "Deployment" Phase (that contains confirmation of the incident) as being independent of the physical and digital investigation. In practice, it appears impossible to confirm a digital crime unless some initial physical and digital investigation is conducted. Baryamureeba and Tushabe (2004), despite being in favour of the IDIP, criticise the model for not providing "sufficient specificity" and question the practicality of the model by drawing an analogy to illustrate the problem associated with this model. According to the analogy, the primary crime scene is where the crime is initiated; the target of the malicious activity is the victim's location which is the secondary crime investigation. The physical and digital investigation processes of Carrier and Spafford's model do not include the secondary crime scene. The fact that the malicious activity is not included in the physical or digital investigation can have a negative effect on the possible reconstruction of a sequence of events. Therefore, according to Kohn et al. (2013), this can lead to incomplete findings in the report presented to the relevant audience. However, this criticism is invalid on the basis that other authors such as Mercuri (2005) and Reith et al. (2002), as cited by Adams (2012), concur that the approach for acquiring digital evidence is essentially the same as that employed in terms of acquiring traditional evidence. Other authors such as Saferstein (2010) and Boddington et al. (2008) approve of Carrier and Spafford's approach by drawing a fundamental similarity between the physical and digital crime scene domains.

Rogers et al. (2006) have also criticised the IDIP stating that despite the fact that this model might be appropriate for investigations where the entire investigative process needs to be followed, the time limitations of certain investigations such as child abduction makes the model infeasible. However, this criticism appears to be in sharp contrast with Baryamureeba and Tushabe's (2004) commendation in relation to the IDIP. Baryamureeba and Tushabe (2004) state that due to the fact that the IDIP has emphasized the reconstruction of events that have led to the incident and focused on reviewing the entire task, this will untimely build a mechanism for swifter forensic

examinations (Baryamureeba and Tushabe, 2004). Moreover, courts often require investigators to conduct a digital investigation using a methodical process in order that courts can assess the reliability of digital evidence presented to them. This means that the notion of swift data examination and analysis suggested by Rogers et al. (2006) in itself is very likely to attract serious challenges by courts (Adams, 2012).

Content was removed for copyright reasons.
Carrier, B. and Spafford, E. (2003). 'Getting Physical with the Digital Investigation Process', *International Journal of Digital Evidence*, 2(2), pp.1–20.

Figure 3. The IDIP after Carrier and Spafford (2003)

Although some criticisms have been levied upon the IDIP, many researchers (Montasari et al, 2015; Valjarevic and Venter 2015; Adams et al, 2014; Kohn et al, 2013; Casey, 2011) have adopted many of the ideas introduced by the model, especially the concept of "digital crime scene". The major and novel contribution of the IDIP is the introduction of the concept of the interaction with "physical investigation". Another main benefit of the model is due to the fact that it has demonstrated well the investigative process, such as Data Collection, Interrogation, Analysis and Reporting.

Based on the Beebe and Clark criteria, the IDIP has only met Requirement 4. The model cannot be said has achieved scientific rigor and relevance as it is not comprehensive, in that it is missing lower-level components (Requirement 1). Also, since the model is not hierarchical, it has not achieved complex process simplification (Requirement 2). The model has not met the level of granularity specified by Beebe and Clark (2005) as it has not incorporated lower layers (Requirement 3). However, the IDIP has been able to delineate standard assumptions, concepts, values, and practices through the use of constraints, definitions and principles (Requirement 4). The Beebe and Clark score given to the IDIP is 1/4.

According to their own five-point criteria, the model is based on the existing theory for physical crime investigations as it has clearly established the interaction between the physical and digital scenes (Requirement 1). The IDIP is also general in terms of technology (Requirement 3) and is specific enough to allow for the technology to be employed to aid the investigators (Requirement 4). Moreover, the model is generic in that it can be applied to both law enforcement and corporate investigations (Requirement 5). The model's practicality however is not clear and has come under criticisms (Beebe and Clark, 2005). The Carrier and Spafford score given to this model is 4/5.

In relation to the Daubert Test, the IDIP has met Requirements 2 and 5. Although the model has been applied to case studies, it has not been tested by its intended user community (Requirement 1); therefore, its potential error rate is not known (Requirement 3). There is also no evidence of any standard associated with this model (Requirement 4). However, the model has been peer-reviewed and published (Requirement 2), and widely accepted and referenced in the digital forensic community (Requirement 5). The Daubert Test score given to the IDIP is 2/5.

2.7.5 Baryamureeba and Tushabe's EDIPM

The Enhanced Digital Investigation Process Model proposed by Baryamureeba and Tushabe (2004) is based on the original model developed by Carrier and Spafford (2003). The EDIPM follows the same principle in that the digital investigation is treated the same as the physical investigation. The model consists of five Phases including: Readiness, Deployment, Trace Back, Dynamite and Review as shown in Figure 4. As with Carrier and Spafford's (2003) IDIP model, the EDIPM incorporates the physical crime scene. However, unlike the IDIP, this model separates the investigation at the 'primary' and 'secondary' crime scenes while representing the phases as iterative rather than linear. Moreover, Baryamureeba and Tushabe (2004) drops the two 'Reconstruction' Phases proposed in Carrier and Spafford's (2003) model, which they claim can result in inconsistency, and instead propose a new Phase, namely the "Traceback" Phase. This new Phase is intended to enable the investigators to trace back to the previous phases in the investigation. The remaining phases included in the EDIPM are the same as those in IDIP. The EDIPM consists of 5 Phases

including: Readiness, Deployment, Trace Back, Dynamite and Review. Figure 4 is the graphical representation of the EDIPM. Figure 4 is the graphical representation of the EDIPM.

Content was removed for copyright reasons.
Baryamureeba, V. and Tushabe, F. (2004). 'The Enhanced Digital Investigation Process Model', *4th Digital Forensic Research Workshop*, pp. 1-9.

Figure 4. The EDIPM after Baryamureeba (2004)

Although Baryamureeba and Tushabe (2004) claim that their EDIPM is an enhanced version of the Carrier and Spafford's (2003) IDIP, they have added little to the IDIP. In fact, this model is not as rigorous as that of Carrier and Spafford's. The EDIPM is aimed at only the field of incident response and neglect the domain of law enforcement. Adams (2012) criticises this model for the ambiguous definitions of the activities in the model such as the terms "multiple analysis" and "synchronised", for which no explanations are provided and which do not have clear meaning in the context of "Analysis". Similarly, Perumal (2009) takes issue with the EDIPM as it is missing necessary investigative Principles such as 'Chain of Custody'. Another shortcoming of this model is that it has not been tested by the experts in the field or applied to any case study.

In relation to the Beebe and Clark criteria, the EDIPM has not met any of the four requirements. The model does not have scientific rigor or relevance (Requirement 1), nor has it incorporated enough details or allowed for the model to be infused with additional layers of details (Requirement 3). The model also does not include investigative Principles, and the description provided for some of its components are not clear (Requirement 4). The Beebe and Clark score given to this model is 0/4.

Based on the Carrier and Spafford five-point requirement, the EDIPM has only met Requirement 1 by providing a relationship between the physical and digital investigations. The model is not practical as it has not been tested to determine its practicality (Requirement 2), nor is it technologically neutral as it has focused on incident response (Requirement 3). Also, the lack of guidance in its application, and its ambiguous descriptions have prevented the design of technological tools to aid DFIs. Moreover, the EDIPM is not applicable to various user communities as its only focus is on the field of incident response. The Carrier and Spafford score given to this model is 1/5.

Regarding the Daubert Test, the EDIPM has only met one of the five requirements, in that it has been subjected to peer-review and publication (Requirement 2). The EDIPM has not been tested by its intended user community (Requirement 1); thus, its potential error rate is not known (Requirement 3). There is also no evidence suggesting that the model has been based on a particular standard (Requirement 4). In addition, the model appears not to have been widely accepted by the digital forensic community (Requirement 5) as there has been no further development of the model since it was first published. The Daubert Test given to this model is 1/5.

2.7.6 Ciardhuáin's EMCI

An Extended Model of Cybercrime Investigation (EMCI) proposed by Ciardhuáin (2004) is the most comprehensive DFIPM presented to date. Ciardhuáin (2004) merges the previously proposed models and extends them by addressing certain activities not incorporated into the previous models. Ciardhuáin's proposed model includes thirteen activities, as shown in Figure 5 in order to model the whole "Information Flow" pertaining to a digital forensic investigation. The EMCI has a linear representation, where the Processes follow the waterfall model allowing the investigators to backtrack to certain Processes if needed. Ciardhuáin takes issue with certain previous models, such as Reith et al's (2002) model, and their lack of explicit mentioning of "Chain of Custody" (Adams, 2012). He considers the Chain of Custody as an instance of Information Flow and argues that the Chain of Custody should be created by those who have handled a piece of evidence and must pass it from one stage to the next, with names added at each step.

Content was removed for copyright reasons.

Ciardhuáin, O. (2004). 'An Extended Model of Cybercrime Investigations', *International Journal of Digital Evidence*, 3(1), pp. 1-22.

Figure 5. The EMCI after Ciardhuáin (2004)

The main contribution of the EMCI is the fact that the model explicitly captures the "Information Flows" in an investigation (from the moment incident is detected until the investigation is concluded.) as opposed to only the processing of evidence. One of the weaknesses of this model is the fact that it has excluded certain important steps such as the return or destruction of digital evidence at the end of investigation. Another shortcoming of this model lies in the fact that the terminology used to describe each activity is not clearly defined (Casey, 2011). For instance, it is ambiguous whether Ciardhuáin (2004) discounts the "Preservation" step since it is not regarded necessary, or because it is considered as part of the "Acquisition" Process. Casey (2011) has also criticised this model for not defining goals (an important requirement) within each step in an investigation. Thus, various users of the model might take different approaches at each stage of a digital investigation, possibly infringing on important forensic principles.

In relation to the Beebe and Clark criteria, the EMCI has achieved Requirements 2 and 4 and Requirement 1 partially. Although the model is comprehensive in capturing the entire investigative process, this is limited only to higher-order process (single-layer details). The EMCI does not provide the lower-level details needed to guide DFIs (Requirement 1). The model has successfully simplified the complex investigative process due to its high-order Processes (Requirement 2). However, the EMCI does not contain the lower-level details needed to retain enough granularity to take advantage of

the model in unique situations (Requirement 3). The EMCI defines standard assumptions and concepts such as 'Information Flow' through the employment of constraints, even though the definitions provided in the model have been criticised by Casey (2011) for their ambiguity. The Beebe and Clark score for the EMCI is 2.5/4.

With regards to the Carrier and Spafford criteria, this model meets all five requirements. It has basis in the existing physical crime scene (Requirement 1); the model appears to be practical enough as it has been tested by its intended user community (Requirement 2). It is also technologically neutral (Requirement 3), and appears to be capable of identifying opportunities for development and deployment of technology to aid the work of DFIs (Requirement 4). The model is also generic enough to be applied in both law enforcement and industry.

Concerning the Daubert Test, the EMCI meets the first three requirements. The model has been tested by DFIs operating within the law enforcement. However, as the author himself identifies the need, the EMCI will also need to be tested in other environments that the model has claimed to cover such as auditing, civil litigation, investigations by system administrators and judicial inquiries. The EMCI has been subjected to peer-review and publication (Requirement 2) and its potential error rate appears to be known due to the model having been tested by experts (Requirement 3). For instance, investigators participating in the testing of the EMCI state that no major elements have been omitted from the model. However, the investigators have felt that there have been activities not normally identified as being separate from other investigative Processes, and some of these were considered as irrelevant for their work, namely Awareness, Transport, Storage and Dissemination (Ciardhuáin, 2004). The investigators have further stated that there must be tighter control on flow of the information to avoid "information leakage" due to the needs for confidentiality required of them by external policies, regulation and legislation. The EMCI does not, however, appear to have been widely accepted within the digital forensic field as it has not been further developed since its creation (Requirement 4). There does not also appear to be any evidence suggesting that the model has adhered to a particular standard (Requirement 5). The Daubert Test given to the EMCI is 3/4.

2.7.7 Rogers' DCSA

The Digital Crime Scene Analysis (DCSA) model proposed by Rogers (2004) builds upon the relationships between the digital and physical investigations as first proposed by Carrier and Spafford (2003) and further supported by Baryamureeba and Tushabe (2004). Rogers (2004), as cited by Adams (2012), acknowledges the contribution of the previous models in particular that developed by Carrier and Spafford (2003). However, Rogers argues that "...what is still lacking is an applied/practical approach to dealing with digital crime scenes and the digital evidence contained therein" (Adams, 2012). Rogers (2004), also cited by Adams (2012), criticizes previous models arguing that they have mainly focused on incident response and neglected important aspects of law enforcement activities such as 'Chain of Custody' and the need to adhere to relevant rules. He states that a model should include a discrete element in relation to the Chain of Custody as this Principle becomes very important when the case is brought to a court of law. This criticism is levied against those authors, such as Reith et al. (2002), who argue that although their models do not include a distinct Phase for the chain of custody, this is implied as part of their models.

Rogers (2004) further criticises previous models by arguing that they envisage one person to have all the required skills to acquire digital data from all the digital sources such as hard disks, routers and networks. He states that this is not the case in non-digital forensic investigations where different specialists will be involved in specific areas of evidence gathering such as fingerprinting and DNA material (Adams, 2012). This argument is valid on the basis that the technology is rapidly changing and therefore expecting one individual to have all the necessary skills in all areas of digital data acquisition appears to be unrealistic. This argument is further validated by ISO/IEC 2037 (2012), where investigators with particular skills are assigned different roles and responsibilities. The novel contribution of the DCSA is the notion of "Forensically Sound Tasks" that result from "properties" of digital forensics and that consist of Authenticity, Chain of Custody, Integrity, Minimization and Reproducibility.

Adams (2012) criticises the DCSA for the fact that separate tasks have been developed for "what could realistically be one task in practice", namely "Survey the Scene" and "Document the Scene". Such criticism is invalid on the basis that in order to achieve

complex process simplification as suggested by Beebe and Clark (2005), a model's components will need to be broken down to assist its intended users in understanding the activities contained in the model more clearly. This criticism is further invalidated given that Adams (2012) goes on to adopt the same approach that he has criticised the DCSA for, in his own model (discussed later), where "Survey the Scene" and "Documentation" are two separate activities at the crime scene.

In relation to the Beebe and Clark criteria, the DCSA meets all the requirements except Requirement 1. The model does not have scientific rigor or relevance as it does not cover the entire investigative process, focusing only on the Analysis stage (Requirement 1). However, the DCSA has simplified the complex investigative process (Requirement 2). Although the model does not contain sufficient layers of details as it stands, it allows for the model to be filled with further components (Requirement 3). Rogers (2004) has also delineated standard assumptions, concepts, value and practices in his model (Requirement 5). The Beebe and Clark score given to the DCSA is 3/4.

Based on the Carrier and Spafford criteria, the DCSA has achieved all of the requirements with the exception of Requirement 4. The model has basis in existing theory for physical crime investigations (Requirement 2). It is not restricted to a specific technology (Requirement 3) and has sufficient details to allow for the creation of technical aids (Requirement 4). The DCSA is also applicable to various fields of digital forensics (Requirement 5). However, it is not clear whether or not the DCSA matches the steps taken in actual investigations as it has not been tested by its user community (Requirement 2). The Carrier and Spafford score given to the DCSA is 4/5.

With regards to the Daubert Test, the DCSA has only met Requirement 2, being the fact that it has been peer-reviewed and published. The model has not been tested (Requirement 1); therefore, its potential error rate cannot be determined (Requirement 3). Also, there does not exist an evidence of any standard that governs the DCSA's operation (Requirement 4). Moreover, the model has not been widely accepted in the digital forensic community (Requirement 5). The Daubert Test given to the DCSA is 1/4.

2.7.8 Beebe and Clark's HOBFDIP

Beebe and Clark (2005) state that previous models lack the detail required to be of practical use; hence they proposed their model to focus on the lower-level activities of a digital investigation as opposed to abstract concepts. This model consists of six Phases as illustrated in Figure 6.

Content was removed for copyright reasons.
Beebe, N. and Clark, J. (2005). 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process', *Digital Investigation*, 2(2), pp.147–167.

Figure 6. The HOBFDIP after Beebe and Clark (2005)

At a first glance, it appears that this model has not built upon the previous models due to its common Phases. However, upon a closer inspection of Beebe and Clark's paper, it becomes clear that Beebe and Clark have provided lower-level details for the Analysis Phase even though the details are not incorporated into the graphical representation of the model. Beebe and Clark's model consists of Phases, Principles and Objectives. Phases are sequential, time-based and distinct in the process, whereas Principles are high-level procedures that apply to more than one Phase while Objectives are the intended outcomes. There are various shortcomings associated with Beebe and Clark's (2005) "Hierarchical, Objectives Based Framework for the Digital Investigation Process" as identified by the authors themselves. These include:

- Its proposed set of Objectives is incomplete.
- The model needs to be expanded upon so that it can also be applied across various layers of abstraction as well as to various types of digital devices.

Other shortcomings of the HOBFDIP include the fact that its lower-level details are only restricted to an initial Sub-Phase structure for the Data Analysis Process. No additional layers of detail have been provided for other Processes in the model. Also, the model is not generic as it is biased towards 'network forensics'. It has incorporated Phases that are often used in the context of incident response such as 'network

monitoring'. Moreover, although the model has been applied to two different case studies as part of its evaluation, no independent testing of the model has been carried out by its intended user community. The notable contribution of this model is the concept of a "multi-tiered" approach, as opposed to the "single-layer" approach identified in the previous models. Another contribution of this model is the introduction of "Principles" that should be applied throughout the investigative process such as "Information Flow", "Documentation" and "Evidence Preservation" even though these Principles had been previously covered in Ciardhuáin's (2004); Mandia et al. (2003); Carrier and Spafford (2003); Reith et al. (2002); Palmer (2001); Ashcroft, (2001).

Based on their own four-point requirement, the HOBFDIP meets the first Requirement partially as its lower-level details are restricted only to the Analysis Process. However, Requirements 2 and 3 are fulfilled as complex investigative process appears to have been simplified even though there is no evidence of the model's application in real practice. The HOBFDIP is also capable of being expanded and being infused with further granularity. Requirement 4, however, has been partially fulfilled as there are some ambiguities in relation to definitions and some task hierarchies. The Beebe and Clark score for the HOBFDIP is 3/4 as it has only partially met Requirements 1 and 4.

In relation to the Carrier and Spafford five-point requirement, the HOBFDIP meets the first Requirement as it has basis in existing physical crime scene investigatory theory. In terms of Requirement 2, although Beebe and Clark argue that their model has practicality due to its level of details, there is no way of determining whether or not the model is actually practical, as it has not been tested by its user community. The model does not also meet the third Requirement as it is not technologically neutral since its emphasis is on the network forensics (The authors themselves admit that their model needs to be expanded to cover different types of digital devices.). However, the HOBFDIP fulfils Requirement 4 as its level of detail, even though incomplete, allows for the addition of specific requirements and gap analysis activities. Similarly, the fifth Requirement is met by this model as it is applicable to both law enforcement and industry. The Carrier and Spafford score for this model is 3/5.

In terms of the Daubert Test, the HOBFDIP does not meet Requirement 1 as there is no evidence suggesting that it has been tested by its intended user community, nor is the

model's potential error rate known as it has not been tested independently. Also, there is no evidence of the model being associated with any standard or recognised guidelines. However, the HOBFDIP appears to have been accepted within the digital forensic community as it is widely referenced. The Daubert Test score for the HOBFDIP is 2/5 as it has partially met Requirements 1 and 4.

2.7.9 Kent et al's FSFP

Kent et al. (2006) created a guideline, the aim of which is to enable the organisations to develop their own digital forensic capability through IT professionals for security incident response. Although the authors state that each organisation should employ the most suitable model based on their own requirements, they go on to propose a high-level model, namely "Four Step Forensic Process", consisting of four stages including: Collection, Examination, Analysis and Reporting. Kent et al. (2006) consider the four steps as common stages of investigative process that have been derived from the previous models stating that the only difference is the level of details provided for each stage. Figure 7 is the graphical representation of this model. The FSFP is simple compared to those proposed by Ciardhuáin (2004) and Reith et al. (2002); however, Kent et al. (2006) delve into some details when describing different activities related to each of the four stages of the model.

Content was removed for copyright reasons.
Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. U.S. Department of Commerce. Available at: http://cybersd.com/sec2/800-86Summary.pdf (Accessed: 16 June 2016).

Figure 7. The FSFP after Kent et al. (2006)

The FSFP has some merits but also some serious flaws. Its strength lies in that fact that it has provided a large amount of background details to enable the organisations to build a general ability in relation to training, procedures and resources. The model also provides some useful details in terms of the standard forensic procedures that could help

the organisations to develop their incident response abilities. However, the FSFP has started from the middle part of the investigative process and misses out the preliminary activities, such as confirmation in relation to whether or not DFIs are authorised to initiate an investigation, and an initial Planning stage which is often followed by Preparation and attendance at the crime scene (Montasari et al, 2015; Adams et al, 2014). The model is also missing some post-data acquisition stages such as Interpretation, Event Reconstruction, Presentation and Investigation Closure, which are required as part of a complete investigative process.

Further shortcoming of the FSFP is due to the fact that the activities specified for each stage are not explicitly represented in the graphical representation of the model but discussed in the text. This significantly reduces the practicality of the model as DFIs would have no visual sighting of the activities that are not presented in the model if they were to adopt it. One might argue that in that case the investigators could simply follow text; however, the counter-argument would be that this would be time-consuming given the scarcity of time imposed by issues such as authorisation or resources. Moreover, this is in opposition to the complex process simplification requirement proposed by Beebe and Clark (2005) which requires the model to be detailed to assist the investigators when undertaking investigations. The model has also inappropriately placed the correct set of activities into the incorrect groups, and in some cases the activities would need to be considered as separate and distinct 'Processes' on their own. For example, the Examination stage contains three activities including: "Develop a plan to acquire the data", "Acquire the data" and "Verify the integrity of the data". Planning and Data Acquisition must be treated as two separate Processes on their own, given that each has a unique aim, a view supported by (Montasari et al, 2015; Valjarevic and Venter, 2015; Kohn et al, 2013; Casey, 2011). Therefore, the absence of a clear structure as well as the lack of important activities in relation to both 'pre-data' and 'post-data' acquisition significantly reduce the practicality of the model.

In relation to the Beebe and Clark criteria, the FSFP does not meet the first two Requirements as the model is not structured (Requirement 1), and its higher-order stages have not been divided into additional layers to facilitate the complex process simplification (Requirement 2). Although the model does not contain any granularity, it allows for the investigating organisations to adjust its details (explained in the text) to

match the organisations' requirements (Requirement 3). Moreover, the model is capable of defining some details to assist organisations in developing their digital forensic capability for security incident response (Requirement 4). The Beebe and Clark score given to this model is 2/4.

With regards to the Carrier and Spafford criteria, the FSFP meets Requirements 1, 3 and 4. The model is based on physical investigation as well as digital investigation (Requirement 1), and it is not dependent on any specific technology (Requirement 3). The model is also specific enough to facilitate technology requirement development (Requirement 4). However, the FSFP is not practical due to missing out essential stages of the investigative process as well as incorrectly grouping its activities (Requirement 2). Moreover, the model is not generic as it only focuses on the domain of incident response (Requirement 5). The Carrier and Spafford score given to this model is 3/5.

In terms of the Daubert Test, the FSFP has not met any of the requirements as the model has not been tested by experts in the field, nor has it been subjected to scientific peer-review or publication. Its potential error rate is also unknown as no testing has been carried out on the model, and there is no evidence suggesting that the model has been influenced by any standard. The model has not also been widely accepted in the digital forensic community. The Daubert Test score given to this model is 0/5.

2.7.10 Kohn et al's FDFI

Kohn et al. (2006) proposed a three-stage "Framework for a Digital Forensic Investigation", that consists of three Phases: Preparation, Investigation and Presentation as presented in Figure 8.

Content was removed for copyright reasons.
Kohn, M., Eloff, J. and Olivier, M. (2006). 'Framework for a Digital Forensic Investigation', *Information Security South Africa Conference*, pp. 1-7.

Figure 8. The FDFI after Kohn et al. (2006)

The FDFI is simply the integration and adoption of the previously proposed frameworks. According to the authors, the purpose of the framework is to provide a clear, step-by-step guide for the acquisition of evidence appropriate for presentation in courts of law. The major drawback of the FDFI is the fact that it is a very high-level approach without providing sufficient details to assist investigators in conducting DFIs. As a result, this has significantly reduced its usability. Although this framework has not made any new contribution (as no new steps are added in the framework), the authors have nevertheless described the importance of the legal requirements associated with the investigative process that the existing frameworks often neglect.

In relation to the Beebe and Clark criteria, the FDFI meets only Requirements 2 and 4. The framework is simple enough to be followed (Requirement 2); also, the descriptions of the Phases are accurate and the authors have highlighted one of the important investigative Principles, namely the Legal Requirements (Requirement 4). However, the framework cannot be considered scientifically rigorous or relevant as it has omitted essential investigative Processes (Requirement 1). Also, the FDFI does not meet granularity requirement as it is simply a high-level framework (Requirement 3). The Beebe and Clark score given to this framework is 2/4.

With regards to the Carrier and Spafford criteria, the FDFI meets the first three Requirements. It has basis in existing physical crime scene theory, and it appears to be practical even though it has not been tested by experts simply due to its very high-level structure (Requirement 2). Moreover, the framework is technologically neutral without being limited to a specific technology (Requirement 3). However, the absence of granularity hinders the development of technology to aid the framework's implementation (Requirement 4). This framework is not also applicable to various domains of digital forensics (Requirement 5). The Carrier and Spafford score given to this framework is 3/5.

Concerning the Daubert Test, the FDFI meets only Requirement 2 as it has been peer-reviewed and published. The framework has not been tested (Requirement 1), thus its potential error rate cannot be determined (Requirement 3). In addition, there is no evidence that this framework is based on any standard. Although Kohn et al. (2006) refer to ISO 17799 and COBIT, they do not draw upon the content of these standards.

They simply state that all organisations (those within South Africa) must have these standards as well as their own policies and procedures in place so that these can assist them in digital investigations (Requirement 4). Furthermore, there is no evidence showing that the framework has been widely accepted in the field of digital forensics (Requirement 5) even though the authors developed the framework further in Kohn et al. (2013) (discussed later). The Daubert Test score given to this framework is 1/5.

2.7.11 Rogers et al's CFFTPM

Computer Forensics Field Triage Process Model (CFFTPM) proposed by Rogers et al. (2006) uses Phases extracted from the Carrier and Spafford's (2003) IDIP. The CFFTPM includes six Phases as shown in Figure 9.

Content was removed for copyright reasons.
Rogers, M., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006). 'Computer Forensics Field Triage Process Model', *Conference on Digital Forensics, Security and Law*, pp. 27-40.

Figure 9. The CFFTPM after Rogers et al. (2006)

The advantage of the CFFTPM is due to its practical and pragmatic approach being developed in reverse of the previous DFIPMs. Rogers et al. (2006) state that the model's procedures used onsite are forensically sound and maintain the Chain of Custody. There is, however, no explicit graphical representation of this important principle, nor is there any description of how the Chain of Custody should be maintained by DFIs. This model is only appropriate for circumstances where a swift examination would need to be conducted at the crime scene. This model should only be used "where appropriate and only after carefully weighing the legal and technical considerations associated with digital investigations". The authors have claimed that this model is suitable in diverse cases as financial fraud, identity theft, cyber stalking and murder making reference to the model's six primary Phases (Planning, Triage, User Usage Profiles, Chronology Timeline, Internet, and Case Specific). However, the model has not been tested in relation to cases involving the stated crimes.

The authors claim that the CFFTPM has been used in real life cases and that the evidence derived through the use of this model has not been challenged by the courts where it has been introduced. However, in relation to the admissibility of evidence derived through the use of this model by courts of law, a question arises as to how the case can be developed against a defendant when the model has missed some very important stages. The CFFTPM lacks Processes such as "Event Reconstruction" or "Interpretation", during which a sequence of events is constructed to answer questions such as who, how, when, why and where. The novel contribution of the Cyber Forensics Field Triage Process Model is that it has moved away from the traditional digital forensic approach of seizing a digital device, transporting it to the lab, making a forensic image, and then searching the entire system for potential evidence. The CFFTPM's focus is to enable DFIs to carry out 'onsite triage' to examine and analyse digital devices within hours as opposed to weeks or months. One of the main shortcomings of this model is that it is not generic as it is only applicable to the law enforcement agencies.

In relation to the Beebe and Clark criteria, the CFFTPM has partially met the first requirement. The model has achieved both relevance and rigor in the sense that it has provided various Sub-Phases or tasks under each primary Phase even though they need to be modified based on the specifics of each investigation. However, the model is not comprehensive and hence incomplete as it is missing various important stages of an investigative process including Readiness, Incident Detection, Preparation, DFL Examination and Analysis, Reporting, Presentation and Investigation Closure. A complete digital investigative process should start from the point where the incident or crime is detected up to and including a point where the result of the investigation is presented to the relevant audience and the investigation is formally closed.

Rogers et al. (2006) state that their model does not negate the capacity for a digital device to be transported back to a DFL for detailed examination and analysis after the initial onsite triage has been carried out. However, they have not expanded on their models to provide additional components associated with post-data acquisition stage in a DFL. Moreover, the authors have not explicitly incorporated any of the investigative Principles into the model even though they have stated that Chain of Custody must be maintained. Thus, as the model stands in its current state, it is incomplete. The

CFFTPM meets Requirement 2 as the authors have been able to simplify the process associated with the Onsite Triage. However, it is not clear whether the authors would have been able to do the same complex process simplification, had they decided to include other investigative Processes in their model. In relation to Requirement 3, the authors have been able to provide sufficient granularity for what they have attempted to achieve (onsite examination and analysis). The CFFTPM has gone deep enough into some detailed components such as "Usage User Profiles", "Chronology Timeline", "Browsing Activities" and "Case Specifics". In terms of Requirement 3, the CFFTPM has met its criteria, i.e. it has provided constraints and definitions, and has objectives and task hierarchies to some extent, despite the fact that the model is missing investigative principles. The Beebe and Clark score for the CFFTPM is 3.5/4 as it has partially met Requirement 1.

In relation to the Carrier and Spafford criteria, the CFFTPM meets Requirements 1, 2, 3 and 4. The authors have clearly demonstrated that their model is based on physical crime scene investigation, since the onsite triage activities outlined in the model are implemented at the crime scene (Requirement 1). The model is also practical matching the steps taken in actual investigations (Requirement 2). It is not limited to a particular tool or technology (Requirement 3). The CFFTPM also has sufficient details to facilitate the development of technical aids (Requirement 4). However, the model does not meet Requirement 5. Although Rogers et al. (2006) state that their model is general enough to be employed across a wide spectrum of investigations, it is only applicable to law enforcement investigations as the investigative approaches that were used to develop this model were derived primarily from child pornography cases. The Carrier and Spafford score for the CFFTPM is 4/5.

With regards to the Daubert Test, the CFFTPM meets all the criteria with the exception of requirement 5. The model has been tested by various State and Local Law Enforcement Officers from Southern Indiana, USA (Requirement 1). The model has also been subjected to peer review and publication (Requirement 2). Moreover, the CFFTPM's error rates appear to have been identified (Requirement 3) since the model has been used in some real-world cases, and the evidence acquired from these cases has not been challenged in the court proceedings where it has been introduced. The CFFTPM has also been associated with some standards as it has complied with the

United States Federal and State rules for the admissibility of evidence (Requirement 4). However, there is no evidence that this model has been widely accepted by the digital forensic community; thus, it does not meet Requirement 5. The Daubert Test Score given to the CFTTPM is 4/5.

2.7.12 Freiling and Schwittay's CPMIRCF

Freiling and Schwittay (2007) proposed "A Common Process Model for Incident Response and Computer Forensics" (CPMIRCF), where the authors make a distinction between digital forensics and incident response, consistent with the view expressed by Mandia et al. (2003). Freiling and Schwittay argue that incident response should focus on the activities of organisations who have been subjected to security breaches with the main aim of quick detection, containment and recovery. In contrast, digital forensics should be utilised to deal with acquiring, analysing and presenting digital evidence by using proven techniques and principles. Although Freiling and Schwittay distinguish between incident response and digital forensics, they argue that these two fields should not be treated separately as there are many common elements between the two different environments. Therefore, Freiling and Schwittay propose a model aimed at both incident response and digital forensics. The CPMIRCF consists of three main Phases including: Pre-Analysis, Analysis and Post-Analysis.

The Pre-Analysis Phase of the model contains three Sub-Phases dealing with steps and activities that are carried out prior to the actual analysis beginning. The Analysis Phase contains five Sub-Phases dealing with the actual analysis while the Post-Analysis Phase is concerned with the documentation of the entire activities performed during the investigation. This model has introduced a new component, Live Response, which is not explicitly mentioned in many of the previous process models. The Live Response element is concerned with collecting information about an incident on hosts that are still running i.e. live. The main drawback of this model pertains to the terminology, and the descriptions of the model's components which are in contrast with other previous models. For instance, the term Analysis is often used by the authors of DFPMs to describe the process of analysing the digital evidence after it has been acquired and examined (Casey, 2004; Reith et al, 2002; Palmer et al, 2001). For instance, referring to Reith et al. (2002) and Palmer et al. (2001), Adams (2012) state that the term

Analysis is often used by these authors to describe the process of analysing digital evidence after it has been acquired and examined. However, Freiling and Schwittay consider this stage to cover all the activities between the initial incident and the preparation of a report (Adams, 2012). This model has been criticised by Adams (2012) for the fact that the descriptions of its Sub-Phases do not correspond with the stated intention of Freiling and Schwittay to produce a generic model applicable to both incident response and digital forensic Processes. For example, Adams (2012) takes issue with the Incident Detection of this model by stating that the description of this Sub-Phase "... is all about intrusion detection and other aspects of incident response". Adams (2012) further argues that many of the tasks listed within the Initial Response Sub-Phase of the model do not have a generic equivalent, e.g. Network Monitoring, Removing Compromised Hosts and Initialising Packet Filtering. Figure 10 represents Freiling and Schwittay's CPMIRCF.

Content was removed for copyright reasons.
Freiling, C. and Schwittay, B. (2007). 'A Common Process Model for Incident Response and Computer Forensics', *3rd International Conference on IT-Incident Management & IT-Forensics*, pp. 19–40.

Figure 10. The CPMIRCF after Freiling and Schwittay (2007)

Using the Beebe and Clark criteria, the CPMIRCF has not met any of the requirements. The model has no scientific rigor or relevance as it is missing many steps that are part of

an actual investigation, and there is no investigative Principle included in the model. The CPMIRCF has not simplified the complex investigative process and is not multi-layered, thus lacking sufficient details to assist the investigators. Moreover, the components in the model do not have generic equivalent. The Beebe and Clark score given to this model is 0/5.

With regards to the Carrier and Spafford criteria, the CPMIRCF meets only Requirements 3 and 4. The model is not based on existing theory for physical crime scene (Requirement 1), nor is it practical matching the steps taken in actual investigations (Requirement 2). Moreover, the model is not generic as it is not applicable to various fields of digital forensic fields with its main focus being on incident response (Requirement 5). However, the model is technologically neutral (Requirement 3), and it has adequate specificity due to its classification of activities (Requirement 5). The Carrier and Spafford score given to this model is 2/5.

In relation to the Daubert Test, the model has only met Requirement 2 as it has been peer-reviewed and published. However, the model has not been tested; thus, its potential error rate is not known. There is also no evidence of any standard associated with the model or no evidence suggesting that the model is widely accepted in the digital forensic community. The Dauber Test score given to the CPMIRCF is 1/5.

2.7.13 Khatir et al's TDERAPM

Claiming that their model would present a detailed approach, Khatir et al. (2008) proposed an iterative process model, namely the Two-Dimensional Evidence Reliability Amplification Process Model (TDERAPM), consisting of sixteen Sub-Phases grouped into five Phases. The TDERAPM also has four tasks that are "Umbrella Activities" relevant across all the Phases of the model. Figure 11 below graphically represents Khatir et al's (2008) TDERAPM.

Content was removed for copyright reasons.

Khatir, M., Hejazi, M. and Sneiders, E. (2008). 'Two-dimensional evidence reliability amplification process model for digital forensics', *Third International Annual Workshop on Digital Forensics and Incident Analysis*, pp.21–29.

Figure 11. The TDERAPM after Khatir et al. (2008)

From the graphical representation of this model, it appears that the coloured horizontal lines represent the importance and value of each Umbrella Activity within a particular phase (Adams, 2012). However, Khatir et al. (2008) have not provided any information concerning how they have evaluated these measurements or how the units have been assessed, a point originally raised by Adams (2012). The authors have not also provided information on how their four Umbrella Activities should be maintained (Adams, 2012). For example, according to the authors, the Preservation/Authenticity Umbrella Activity is intended to enable the forensic team to follow "...disciplined and fully documented steps". However, no information has been provided concerning what this means and how this is to be achieved in practice (Adams, 2012). Moreover, a trivial discussion is provided in relation to computer tools that can be applied to all aspects of investigative process without further details being provided. In line with the views expressed by other authors (Valjarevic and Venter, 2015; Adams, 2012), it is unnecessary to incorporate into a process model details regarding what digital forensic tools should or should not be used. This might negatively affect the flexibility required by the investigators who should use their own trainings and experience to adopt the correct set of tools.

Other shortcomings of this model relate to aspects of integrity regarding the acquired data and the return of evidence; Khatir et al. (2008) make reference to a table that is absent (Adams, 2012). Furthermore, this model has not taken into account Information Flow, nor has it considered the physical investigation with the exception that it has provided a Sub-Phase for the Physical Evidence Collection. Further shortcomings of the TDERAPM are associated with its discussion of the roles for the two sets of individuals including inspectors and managers that the authors have specified in their paper. According to Khatir et al's (2008) paper, the inspector has the role of performing the practical aspects of the investigation whereas the manager has the role of estimating costs, time and resources and acquiring an idea in relation to the potential results. Adams (2012) criticises such an approach, stating that although this might appear valuable in theory, it will not be practical. Such a criticism is valid on the basis that the model assumes that all the earlier cases have been sufficiently logged and categorised despite no solution being suggested by the authors in their paper (Adams, 2012). Moreover, as Adams (2012) states, each specific case is very likely to have different details from the others. Therefore, stating that the costs or the potential conviction rate can be predicted on the basis of the earlier cases appears to be naïve, in particular if there is no research to rely upon (which is often the case).

Moreover, there are some other statements made by Khatir et al. (2008) that do not reflect the actual digital forensic practice and do not appear to be well researched. For instance, the authors have stated, "The ultimate goal of a digital forensic investigation is to support the prosecution." Although prosecution can be a major element of a digital forensic investigation, this statement is flawed on two accounts. Firstly, the actual goal of a digital investigation is to extract evidence from digital sources to prove or refute an offense (Casey, 2011; Baryamureeba and Tushabe, 2004, Palmer, 2001). Secondly, Khatir et al's (2008) statement has not taken into consideration the circumstances in which the case under investigation might not involve a prosecution (Adams, 2012). For example, in situations where the case has not been serious enough to be referred to law enforcement, there will be no prosecution aspect to the case. In such circumstances, the disciplinary actions will be carried out by company management themselves instead.

Finally, the TDERAPM has not provided a new 'practical' contribution to the existing DFIPMs as its components have been simply derived from the previous models. For

instance, issues associated with legal aspects, authorisation, development of the investigation plan and the team members' selection have been previously covered by Freiling and Schwittay (2007), Brown (2006) and Ciardhuáin (2004). Also, the model would be of no practical value due to the fact that no information is provided in relation to its implementation. The TDERAPM is not also generic as it is aimed only at incident response; this becomes even more obvious through the use of certain statements made by Khatir et al. (2008), themselves, such as the need to reinforce the compromised organisations' security. The main contribution of this paper is the theoretical concept of 'management issues' introduced as an "umbrella activity" and 'Case Management/Team Setup', as opposed to practical process issues.

In relation to the Beebe and Clark (2005), the TDERAPM meets only Requirement 2, where the model has been able to conduct the complex process simplification to some extent through its high-level Phases and Sub-Phases. However, the model has no scientific rigor due to missing many details, which also greatly reduces its scientific relevance (Requirement 1). In terms of the granularity of the model, although it has incorporated Sub-Phases categorised into groups of Phases, these are high-level without providing essential level of details (Requirement 3). The model has also not delineated standard assumptions, concepts, and values in relation to digital forensic practice. The paper has presented many uninformed and flawed discussions as stated while analysing the model with regards to digital forensic practice that are open to challenge (Requirement 4). The Beebe and Clark score given to this model is 1/4.

Based on the Carrier and Spafford criteria, the TDERAPM meets only Requirements 3 as it is technologically neutral (Requirement 3). However, the model has no basis in the existing theory for physical crime scene (Requirement 1). Furthermore, despite the fact that Khatir et al. (2008) have identified key factors of an investigation in a high-level approach, such a high-level approach will be of no practical value, a view supported by Beebe and Clark (2005), since the model is missing essential details (Requirement 3). Therefore, this will significantly constrain the ability to design technology to aid DFIs using the model (Requirement 4). In addition, the TDERAPM is not applicable to all user communities as its only focus is on the field of incident response. The Carrier and Spafford score given to this model is 1/5.

Using the Daubert Test, the TDERAPM meets only Requirement 2 as it has been peer reviewed and published. The model has not been tested (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). Furthermore, there are no standards referenced by or associated with the TDERAPM (Requirement 4), nor is there any evidence suggesting that the model has been widely accepted by the digital forensic community (Requirement 5). The Daubert Test given to this model is 1/5.

2.7.14 Selamat's MPDFIF

Selamat et al. (2008) claimed that they had identified common Phases in the previous models and had mapped them to a "more concise model" to produce a map of digital forensic investigations framework. Five Phases are identified in this model, Mapping Process of Digital Forensic Investigation Framework, including: Preparation, Collection and Preservation, Examination and Analysis, Presentation and Reporting and Disseminating the Case. The authors state that their study of thirteen previous models reveal a number of redundant steps and Processes with different terminologies, and as a result they mapped the previous models in an attempt to simplify those previous complex models.

Contrary to what Selamat et al. (2008) claim, the MPDFIF has various shortcomings. The authors state that their model can be used as a "general digital forensic investigation model for investigating all incident cases without tampering the evidence and protecting the chain of custody". However, upon a closer inspection of the MPDFIF, it becomes evident that this model is far from being applicable to the different fields of digital forensics. For example, certain Phases relevant to the field of commerce that should be incorporated into a generic model are missing in the MPDFIF, such as Forensic Readiness, which is considered to be essential to prepare organisations for a possible incident or a security breach (Valjarevic and Venter, 2015, Montasari et al, 2015, Rowlingson, 2004).

Also, important Phases relevant to the Incident Response such as pre-incident preparation requirements from the "A Common Process Model for Incident Response and Computer Forensics" of Freiling and Schwittay (2007) are missing even though Selamat et al. (2008) claim that their model is based on the integration of the previous

models. The MPDFIF also lacks a graphical representation to assist the investigators in conducting digital investigations. The details associated with each Phase of this model are also very ambiguous, and no investigative principle (such as Obtaining Appropriate Authorisation, Keeping an Audit Trail of all the Activities or Maintaining Chain of Custody) have been considered in the MPDFIF.

In relation to the Beebe and Clark criteria, the MPDFIF does not meet any of the requirements as it has no scientific rigor or relevance. The model also does not have any graphical representation, and as a result there is no complex process simplification associated with it. Moreover, the MPDFIF does not incorporate any level of details, nor are the descriptions of the Phases in the model clear. The Beebe and Clark score given to the MPDFIF is 0/4.

Based on the Carrier and Spafford criteria, the MPDFIF meets only Requirement 3 since it is not dependent on a specific technology. However, the model has no basis in existing physical crime scene theory as there are no activities in the model pertaining to those of physical crime scene (Requirement 1). Since the MPDFIF is also missing some necessary steps of the investigative process and it has not been tested, the model cannot also be considered practical (Requirement 2). The lack of adequate details and clear definitions provided by the authors also prevents the implementation of technology to aid the model's development implementation (Requirement 4). This model is not also generic as it only focuses on the domain of incident response. The Carrier and Spafford score given to the MPDFIF is 1/5.

Using the Daubert Test, the MPDFIF only meets Requirement 1 as it has been peer-reviewed and published. The model has not been tested (Requirement 1); therefore, its potential error rate is not known (Requirement 3). There is also no standard referenced by this model (Requirement 4), nor is there any evidence showing that the model has been widely accepted in the digital forensic community (Requirement 5). The Daubert Test score given to the MPDFIF is 1/5.

2.7.15 Cohen et al's DFPM

Cohen (2009) proposed a Digital Forensic Process Model, that consists of seven Processes including: Identification, Collection, Transportation, Storage, Examination and Traces, Presentation and Destruction. Since the focus of the DFPM is on the examination of digital evidence, it only covers the middle stages of the investigative process. This has led to the model omitting some essential stages of the investigative process including those related to preliminary activities and those associated with post-data acquisition and examination. Some of the preliminary activities that the DFPM is missing include those related to Obtaining Authorisation (Montasari et al, 2015; Ciardhuáin, 2004), Preparing Tools and Techniques (Casey, 2011), Understanding Task Requirements (Adams et al, 2014), Performing Risk Assessment (Montasari, 2016, a and b; Rowlingson, 2004) and selecting the investigative team as well as defining roles and responsibilities (Brown, 2006), etc. The post examination activities that this model is missing include those related to Reporting and Investigation Closure.

The model has also inappropriately placed the Analysis, Interpretation, Attributions and Reconstruction activities under the Examination Process. However, Analysis, Interpretation and Reconstruction activities must be treated as distinct and separate "Processes" (Montasari et al, 2015; Valjarevic and Venter, 2015; Carrier and Spafford, 2003), and Attribution must be treated as a Phase under the Analysis Process (Kohn et al, 2013; Casey, 2011). The main advantage of the DFPM is its inclusion of the Reconstruction stage, which is missing in almost all the previous DFIPMs with the exception of the models proposed by Casey (2011) and Carrier and Spafford (2003). The Reconstruction step in Cohen's (2009) model refers to a set of mechanisms that have given rise to the effect of digital evidence produced. Therefore, according to the model, Reconstruction is a process through which the investigators will need to list certain assumptions and limitations in order to present how evidence came into existence.

Using the Beebe and Clark criteria, the DFPM meets only Requirement 2 and 3 as it is simple enough to be employed and also allows for the model to be infused with further details. The model does not have scientific rigor or relevance due to its omitting important stages of the investigative process and has not been capable of properly

defining its concepts, as its components have been grouped incorrectly. The Beebe and Clark score given to this model is 2/4.

In relation to the Carrier and Spafford criteria, the DFPM meets only Requirements 3 and 5 as it is not dependent on a particular technology (Requirement 3) and also can be applied to the different user communities (Requirement 5). The model has no basis in the theory for physical crime scene investigation (Requirement 1), nor is it practical because it has omitted some essential stages of the investigative process (Requirement 2). The DFPM is not also specific enough to allow for the technology to be used to help the investigators (Requirement 4). The Carrier and Spafford score given to this model is 2/5.

Based on the Daubert Test, the DFPM only meets Requirement 2 as it has been peer-reviewed and published. However, there is no evidence of the model having been tested, its error rate being known, any standard governing its procedures, or it being widely accepted in the digital forensic community. The Daubert Test score given to this model is 1/5.

2.7.16 Yusoff et al's GCFIM

Yusoff et al. (2011) state that they reviewed a selected number of previous models and identified common processes from those models to propose their Generic Computer Forensics Investigation Model. The GCFIM contains the following five stages: Pre-Process, Acquisition and Preservation, Analysis, Presentation and Post-Process as shown in Figure 12.

Content was removed for copyright reasons.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011). 'Common Phases of Computer Forensics Investigation Models', *International Journal of Computer Science & Information Technology*, 3(3), pp. 17-31.

Figure 12. The GCFIM after Yusoff et al. (2011)

Yusoff et al. (2011) claim that their model "would make it easier for new users to understand the processes". However, contrary to such a claim, the model has many shortcomings that in fact question the credibility of such a claim. For instance, in relation to their Pre-Process stage, the authors simply reduce their discussion to the statement that this stage should contain tasks that need to be done prior to the actual investigation. However, Yusoff et al. (2011) do not provide any details of what those tasks are. Moreover, this model misses some essential investigative stages such as the Examination Process, in which data needs to be harvested and reduced so that the investigators can obtain the relevant information that would represent potential digital evidence. Throughout their paper, Yusoff et al. (2011) make certain general statements without elaborating on what they are attempting to convey. For instance, they state that "Various types of analysis are performed on the acquired data to identify the source of crime and ultimately discovering the person responsible of the crime." Such a general statement does not appear to be of any useful value unless "those various types of analysis" are detailed out. The details associated with the five stages the GCFIM are also unclear.

The GCFIM has no new contribution to the field, and the model emerges as identical to the Selamat et al's (2011) MPDFIF, which itself is a repetition of previous research. Since the GCFIM is identical to that of the Selamat et al's (2008) model and because the GCFIM similarly does not provide any results or conclusions, it has not been assessed against the three sets of assessment criteria.

2.7.17 Agarwal et al's SDFIM

Agarwal et al. (2011) proposed their Systematic Digital Forensic Investigation Model (SDFIM) claiming that this model addresses some of the shortcomings of the previous methodologies. The SDFIM is based on the model developed by Palmer (2001) and consists of eleven Phases as shown in the graphical representation of this model in Figure 13 below.

Content was removed for copyright reasons.
Agarwal, A., Gupta, M., Gupta, S. and Gupta, C. (2011). 'Systematic digital forensic investigation model', *International Journal of Computer Science and Security*, 5(1), pp.118–130.

Figure 13. The SDFIM after Agarwal et al. (2011)

- Phase 1 (Preparation) involves acquiring an initial understanding of the nature of the crime and activities and preparing materials for packaging evidence sources.
- Phase 2 (Securing the Scene) deals with securing the crime scene from unauthorized access and preserving the evidence from being contaminated.
- Phase 3 (Survey and Recognition) involves the performance of an initial survey by the investigators for evaluating the scene, identifying potential sources of evidence and formulating an appropriate search plan.
- Phase 4 (Documenting the Scene) involves the documentation of the crime scene along with photographing, sketching and crime-scene mapping.

- Phase 5 (Communication Shielding) involves blocking all possible communication options of the devices prior to conducting evidence collection.
- Phase 6 (Evidence Collection) involves investigators acquiring evidence from digital devices.
- Phase 7 (Preservation) includes packaging, transporting and storing the evidence. During this Phase, investigators must follow appropriate procedures to ensure that the evidence is not altered or destroyed, and all potential sources of evidence must be identified.
- Phase 8 (Examination) involves examining the contents of the acquired evidence by digital forensic analysts and extracting information that is critical for proving the case.
- Phase 9 (Analysis) includes a technical review of the Examination results. Also, establishing relationships between fragments of data, analysing hidden data and reconstructing the event data will need to be conducted during this phase.
- Phase 10 (Presentation) involves presenting the investigation results to the relevant audience.
- Phase 11 (Result and Review) includes reviewing the steps in the investigation and determining areas of improvement.

Citing Pollitt (2007), Agarwal et al. (2011) state that there has been a need for a "standard methodology used for all digital forensics investigations". Agarwal et al. (2011) go on to criticise the previously developed models for being mainly ad-hoc tools, arguing that much needs to be achieved in this particular domain. This argument is valid on its own right given that many other researchers have raised the same issue (Montasari, 2016, a; Montasari et al, 2015, Adams et al., 2014, Cohen, 2012; Cohen et al., 2009; Kent et al, 2006; Beebe and Clark, 2005; Ciardhuáin, 2004; Carrier and Spafford, 2003; Palmer, 2001). However, such common statements will also need to be backed by a solution or at least some steps in the right direction, something which has not been materialized in Aggarwal et al's (2011) model.

A critical analysis of the SDFIM has revealed both shortcomings and inconsistencies in relation to associating various activities to the different Phases of the model (Adams, 2012). Although the activities that Aggarwal et al. (2011) have defined in their model

are correct on their own rights, these activities have been inappropriately associated with the Phases of the model. In other words, the authors have inappropriately related a valid set of activities to the wrong Phases in the model. For instance, activities such as "Developing a Strategy for Investigation" and "Considering Various Technical, Legal and Business Factors" that Aggarwal et al. (2011) have incorrectly associated with the "Preparation" Phase must in fact be related to the Planning stage that this model is missing. Such an argument is in line with the ACPO Good Practice Guide for Digital Evidence (2012), and the approach taken by other researchers including Montasari (2016, a), Casey (2011) and Brown (2006). Thus, the Planning stage should deal with drawing a plan for the aforementioned activities, whereas the Preparation Phase must deal with the 'implementation' of those activities.

Another example of associating a correct activity to a wrong Phase pertains to the requirement for DFAs to create evidence backups during the "Examination" Phase. This must take place during or just after the Data Collection Stage. Aggarwal et al. (2011) have also inappropriately defined the activity, "considering the privacy rights of the suspect" under the Preparation Phase. Firstly, this should not be limited only to the suspects; the consideration for privacy rights of the victims, witnesses, investigators and all the other individuals involved in the investigation are equally important. Secondly, this activity should not be confined to a single point in time as the privacy rights of the individuals involved must be maintained throughout the entire investigation. Therefore, this activity would need to be treated as an 'investigative Principle' as opposed to an "activity".

More examples of the inappropriate placement of activities in the SDFIM concern those of "Formulation of a Search Plan" and "Planning for the Collection and Analysis of Digital Evidence". In the case of the former, this activity has been defined under the "Securing the Scene" Phase. However, considering the time limit often imposed by the search warrant, this activity must be carried out long in advance in the "Planning" stage, that this model lacks, in order to save time. In the case of the latter, similarly this activity, which has also been placed under the "Securing the Scene" Phase, should be defined under the Planning stage, a view supported by Montasari (2016, b and c), and Brown (2006). Furthermore, the activity of the "Identification of Suspects" at the crime scene under the "Securing the Scene" Phase must take place during the "Intelligence

Gathering" Phase, that is also absent in this model, just after the crime has been detected and reported.

Final instances of such misplacement of the activities in the SDFIM pertain to those activities of "Packaging", "Transportation" and "Reporting". The authors have defined the "Packaging" and "Transportation" activities under the model's "Preservation" Phase. However, these activities must be part of the "Collection" stage of the investigative process as outlined in ACPO (2008) and supported by other researchers (Montasari, 2016, c; Adams, 2012). The "Reporting", which has been defined as an "activity" under the "Presentation" stage, should also be a separate Phase on its own right prior to the Presentation Phase. This practice is required by ISO/IEC 27043 (2015) and Montasari (2016, c). In the light of the Preservation Phase itself, this should be considered as both an activity under Securing the Scene Phase as well as one of the Investigations Principles that this model lacks.

Aggarwal et al. (2011) have not also been consistent in terms of their criteria for the categorisation of the model's Phases. Many of the SDFIM's Phases could have been grouped into one single Phase (Adams, 2012). For example, "Survey and Recognition", "Communication Shielding" and "Preservation" Phases should all be placed under the "Securing the Scene" Phase as "Sub-Phases" rather than as separate Phases. This is in accordance with the approach taken by other researchers including: Montasari, (2016, c), Casey (2011), Beebe and Clark (2005) and Carrier and Spafford (2003). Other shortcomings of the model are associated with the vital stages of the investigative process that have been omitted. These include: Incident Detection, First Response, Intelligence Gathering, Planning, Interpretation, Event Reconstruction and Reporting. Also, missing in the model is the 'Investigation Closure' stage, where activities associated with the management of evidence are performed such as its return to the rightful owner, its storage, destruction, or cleansing and reuse, where the dissemination of the investigation is communicated to the relevant stakeholders, and where the results are recorded for the future reference.

The lack of inclusion of Investigative Principles in the SDFIM are further shortcomings of this model. These include: "Addressing Safety Issues", "Maintaining a Chain of Custody" (Kohn et al., 2013; Beebe and Clark, 2005; Carrier and Spafford),

"Maintaining Information Flow" (Montasari, 2016, b and c; Montasari et al., 2015; Ciardhuáin, 2004) and "Maintaining a Case Management" (Adams et al., 2014; Khatir et al, 2008), etc. Although Aggarwal et al. (2011) have identified the need for documentation throughout all the stages of the investigation, they have nevertheless limited this activity only to a single Phase, Documenting the Scene, in their model (Adams, 2012). As much as it is important to document the activities carried out at the crime scene, it is also vital to maintain a detailed documentation of all the other activities performed throughout the entire investigative process. Therefore, Documentation must also stand as an "investigative Principle" in accordance with ACPO (2012), ISO/IEC 27043 (2015) and ISO/IEC 27037 (2012).

Throughout their paper, Aggarwal et al. (2011) have made certain statements regarding both technical issues as well as the description of the model that question the level of diligence that has been put into the background research for the development of their model. In terms of the technical issues, for instance, referring to mobile devices Aggarwal et al. (2011) have stated that the majority of evidence will be of a volatile nature being present in ROM. According to Adams (2012), this statement is inaccurate considering the fact that large amount of evidence contained in mobile devices is non-volatile since most of data is stored in flash memory and therefore is not lost when the mobile device is turned off (Adams, 2012). The authors have also argued that all the potential sources of evidence must be identified during the "Preservation" Phase. Such an approach is also flawed on two accounts. Firstly, the aim of Preservation, as the name suggests, should be to preserve the original state of both the physical and digital evidence in order to avoid altering the state of the evidence. Secondly, the evidence is not identified until digital forensic analysts have started the examination of the acquired data (image) during the Examination stage of the investigative process, a view supported by Kohn et al. (2013), Casey (2011) and Venter (2006).

Moreover, throughout their paper, Aggarwal et al. (2011) have made certain claims without substantiating those claims. For instance, they have argued that their model is standardized without explaining how the model has acquired the "standardization" status. The authors have also claimed that the SDFIM is relevant to both fields of law enforcement and commerce. However, the descriptions provided for the model's activities reflect those carried out within the law enforcement environment. Aggarwal

et al. (2011) have also made certain suggestions in relation to the activities of their model without being specific and detailed. For instance, the authors have stated that investigators will need to protect integrity and minimise the corruption of digital evidence. However, they have not provided any details on how the investigators should achieve such tasks. Thus, this will further question the level of diligence that has been put into developing the model.

Finally, the critical analysis of the SDFIM suggests a cursory approach that the SDFIM's authors have undertaken in designing and developing this model. Aggarwal et al. (2011) themselves have implicitly admitted that their model is not complete, stating that the SDFIM needs to be applied in a "variety of cases" and improved based upon feedback. As a result, they call for other researchers to update the SDFIM by identifying and incorporating "new constraints" into the model.

Using the Beebe and Clark (2005), the SDFIM meets only Requirement 2. Authors of the model has been able to simplify the complex process simplification as the model has included a set of "Phases" and "Activities" even though these components have been misplaced (Requirement 2). The model has no scientific rigor or relevance (Requirement 1), nor does it have sufficient granularity (Requirement 3). Moreover, the model is missing investigative principles and has not provided consistent, accurate descriptions in relation to its components. The Beebe and Clark score given to the SDFIM is 1/4.

In terms of the Carrier and Spafford criteria, the SDFIM meets only Requirements 1 and 3. The model has basis in physical crime scene theory (Requirement 1), and it is not dependent on a specific technology (Requirement 3). However, the SDFIM is not practical as it is missing essential investigative stages (Requirement 2), and the model is not specific enough to facilitate technology requirement development because of inconsistencies in its data flow (Requirement 4). Furthermore, the SDFIM is not generic as its focus is only on the law enforcement environment (Requirement 5). The Carrier and Spafford score given to this model is 2/5.

Based on the Daubert Test, the SDFIM only meets Requirement 2 as it has been subjected to peer review and publication. However, the model has not been tested by its

intended user community (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). Also, there is no standard pertaining to this model. Although Aggarwal et al. (2011) have made a brief reference to the guidelines outlined in the National Institute of Justice, they have not drawn upon any of those guidelines. The authors have simply stated that the NIJ recommends certain types of Analysis activities such as "timeframe analysis, hidden data analysis, application analysis and file analysis of the extracted data" without incorporating any of the guidelines into their model (Requirement 4). Also, there is no evidence suggesting that the SDFIM has been widely accepted in the digital forensic community (Requirement 5). The Daubert Test score given to this model is 1/5.

2.7.18 Valjarevic and Venter's HDFIPM

Based on the belief that "there is currently no harmonised digital forensic investigation process model", Valjarevic and Venter (2012) proposed a model entitled the "Harmonised Digital Forensic Investigation Process Model (HDFIPM)". The concept behind Valjarevic and Venter's (2012) approach in intending to harmonise previous models is praiseworthy especially considering the fact that very few attempts have been previously made to bring some sorts of consistency to the existing models. However, similar to all the other DFIPMs, this model is also far from having achieved the status of "harmonisation" despite the claim made by its authors. Prior to providing the rationale for the view expressed, one would firstly need to examine the meaning of the verb "harmonise". Oxford Dictionary (Oxford Dictionaries, 2016) defines "harmonise" as "make consistent or compatible". Other online dictionaries provide similar definitions as "to bring into harmony, accord, or agreement" (Dictionary.com, 2016), or "bring several things into consonance or relate harmoniously" (TheFreeDictionary, 2016). Based upon the aforementioned definitions and other supporting references (Kohn et al., 2013; Cohen, 2012; Beebe and Clark, 2005; Ciardhuáin, 2004; Reith et al., 2002), it is therefore reasonable to assume that in order to be able to harmonise the existing models, one would need to identify, purify and merge the common elements (both components and terminology) found in those models.

Until now, no harmonisation has yet taken place in relation to a unified DFIPM as the authors of the DFIPMs have adopted differing approaches in their models. In fact,

Valjarevic and Venter themselves highlight this issue in a later published paper (Valjarevic and Venter, 2015), stating that the existing models are ad-hoc tools because they have been developed by the authors "based on their own personal experience" (Valjarevic and Venter, 2015). In order to bring harmonisation to the existing DFIPMs, there must be a 'synergy' between different points of view as opposed to only the authors' own ideas. In fact, in any scientific field, synergy is required to bring harmony and consistency to difficult concepts. The critical analysis of the HDFIPM reveals that similar to other authors of DFIPMs, Valjarevic and Venter (2012) have also adopted their very own approach to design the model. This is contrary to their claim that the HDFIPM has achieved the status of "harmonisation". The analysis in the following paragraphs provides the rationale for the argument put forward.

As with other authors, Valjarevic and Venter (2012) have adopted their own terminology without following any standard or guidelines such as those outlined in the ACPO (2012) or ISO/IEC 27037 (2012). For instance, the authors have referred to the "investigative Principles" included in their model as "Parallel Actions". This is contrary to the terminology "Overriding Principles", which is commonly recognised by other researchers in the field (Montasari, b and c; Montasari et al., 2015; Montasari, in press; Adams et al., 2014; Beebe and Clark, 2005). Another example relates to missing Phases included in other models that this model lacks such as "Forensic Readiness" (Montasari, c; Kohn et al., 2013; Casey, 2011; Rowlingson, 2004; Carrier and Spafford, 2003; Mandia et al., 2003).

There are various other shortcomings associated with this model including those related to the missing components and investigative Principles, not least the lack of sufficient level of details, as well as the inappropriate classification of the Phases in the model. An example of the incorrect categorisation of the model's Phases pertain to "Potential Evidence Transportation" and "Potential Evidence Storage", which have been assigned two separate Phases. The two components would need to be included under the "Potential Evidence Collection" as two Sub-Phases in accordance with ACPO (2012) and ISO/IEC 27037 (2012), and the approach taken by Montasari (b and c), (Adams, 2012) and Carrier and Spafford (2003).

Examples of missing components concern both 'Phases' and 'investigative Principles'. In terms of missing Phases, the model lacks the 'Forensic Readiness' (as stated above), 'Securing and Evaluating the Crime Scene' (Casey 2011 and 2004; Rogers et al., 2006) 'Interpretation' and 'Event Reconstruction' (Montasari, 2016, b and c; Carrier and Spafford, 2003) and 'Reporting' (Freiling, 2007; Ciardhuáin, 2004; Reith et al., 2002). There are also no activities associated with the management of evidence such as return, cleanse and reuse or destruction of evidence. With regards to missing investigative Principles, the model is missing 'Maintaining a Detailed Information Flow', 'Addressing Safety Issues' and 'Maintaining a Detailed Case Management' (Casey, 2011; Khatir et al., 2008; Ciardhuáin, 2004). More importantly, the HDFIPM lacks sufficient level of details as emphasized by Beebe and Clark (2005) and further supported by Montasari (2016, c). In relation to the lack of granularity associated with the model, the authors, themselves, admit that the model will need additional layers of details, stating "The development of more Sub-Phases on the second tier of the proposed model could also be considered in future research."

Based upon the Beebe and Clark criteria, the HDFIPM meets only Requirement 4 as the descriptions of the Phases are reasonably accurate, and the model has included some investigative principles. However, the model does not have scientific rigor due to missing components (Requirement 1). Also, no complex process simplification has been carried out (Requirement 2). Furthermore, the model also does not provide any granularity since it lacks lower-level details (Requirement 3). The Beebe and Clark score given to this model is 1/5.

Using the Carrier and Spafford criteria, the HDFIPM meets Requirements 1 and 3 as the model is based on physical crime scene theory (Requirement 1), and it is technologically neutral without being limited to a specific technology (Requirement 3). However, the HDFIPM is not practical due to missing important investigative steps (Requirement 2), nor does it have specificity to facilitate technology requirement development due to the absence of granularity in the model (Requirement 4). Also, the intended user community of the model is not clear. It is however obvious that the HDFIPM cannot be applicable to the law enforcement environment as it is missing important stages associated with this domain such as 'Securing and Evaluating the Crime Scene'. A model that is not applicable to all the user community, namely law

enforcement, commerce and incident response, cannot be considered as generic (Requirement 5). The Carrier and Spafford score given to this model is 2/5.

With regards to the Daubert Test criteria, the HDFIPM only meets Requirement 2 as it has been peer reviewed and published. However, the model has not been tested by the experts in its intended user community (Requirement 1); therefore, its potential error rate is unknown (requirement 3). There is also no evidence suggesting that the model has drawn upon any standard (Requirement 4), nor is there any evidence showing that the model has been widely accepted in the digital forensic community. The Daubert Test score given to this model is 1/5.

2.7.19 Kohn et al's IDFPM

Kohn et al. (2013) proposed a Process Flow Diagram consisting of thirty six Sub-Processes grouped into five Processes, namely Preparation, Incident, Incident Response, Digital Forensic Investigation and Presentation. The components of this model have been extracted from the previous models, hence the name Integrated Digital Forensic Process Model (IDFPM). As with Aggarwal et al's (2011) inconsistent criteria for classifying their model's activities as Phases (correct set of activities were placed in incorrect Phases.), Kohn et al. (2013) have also adopted a flawed approach in categorising their model's Sub-Processes as Processes. Although the Sub-Processes related to various Processes of the model are correct in their own right, the criteria for their classification as a Process is erroneous. For instance, the whole of Digital Forensic Investigation Sub-Processes are covered in one single Process. However, these should have been grouped into various separate Processes including: Collection, Examination, Analysis, Interpretation and Event Reconstruction, which would be consistent with the approach taken by other researchers (Beebe and Clark, 2005; Ciardhuáin, 2004; Carrier and Spafford, 2003; Reith et al., 2002). Another example relates to the Sub-Processes in the Presentation Process which should have also been divided into various separate processes such as Reporting, Presentation and Investigation Closure in accordance with ISO/IEC 27043 (2015).

Kohn et al. (2013) have also misplaced various Sub-Processes in their model, which highlights a cursory approach to research into the development of the model. For

instance, the authors have incorrectly placed Communicate and Review in the Digital Forensic Investigation Process before Reporting in the Presentation Process. This is flawed as an investigation must be first finalised and formally resolved before the communication of the results can be made to the relevant stakeholders or before the investigators could embark upon reviewing the whole investigation. Transport and Store Sub-Processes have also been incorrectly placed before the evidence Collection in the model. In circumstance where evidence needs to be acquired at the crime scene, transportation and storage of the evidence will need to be carried out after the data acquisition and not before it (ACPO, 2012; ISO/IEC 27043, 2015; ISO/IEC 27037, 2012). However, these two Sub-Processes have been incorrectly placed before the Collection Sub-Process in the model. This is a serious flaw which can have a severe impact on the investigation since a missing step or a step that has been performed in the wrong order can cause the entire digital investigation to be challenged and ultimately rejected by courts.

The IDFPM also lacks lower-level components as suggested by Beebe and Clark (2005) and further supported by Montasari (2016, c) and Montasari et al. (2015). Although Kohn et al. (2013) have made an attempt to model the whole investigative process, the model still has high-order processes without sufficient level of details. The authors have not provided any lower-level investigative details necessary to guide the steps of investigators. For instance, data collection activity in the IDFPM is simply represented as a Sub-Process "Collect" without providing further details on both 'live' and 'static' data acquisition steps. As a result, this will further bring into question the practicality of the model.

Also, as with almost all the previous models, the "Reporting" in Kohn et al's (2013) IDFPM has not been assigned a single discrete Process; instead it has been inappropriately placed under the Presentation Process as a Sub-Process. Reporting and Presentation have two different aims; in line with ISO/IEC 27043 (2015), the aim of a forensic report should be to compile the investigation findings, whereas the goal of Presentation should be to present those findings. In real practice, Reporting is carried out in advance of the Presentation Process so that the investigators have sufficient time to review the compiled report before its submission to the court or any other relevant audience. Furthermore, the IDFPM is missing some important components such as

those associated with evidence management including return, destruction or reuse of the evidence. The model has not also assigned any components to accommodate for activities associated with identifying and applying the lessons learnt.

Unlike the authors of many of the previous models, Kohn et al. (2013) have distinguished between an investigative Principle and a Process. For instance, the authors have incorporated Documentation as a Principle, which needs to be maintained throughout the other processes in the IDFPM. Although this is a commendable approach, at the same time other important investigative Principles have not been introduced into the model. These include: Preservation of Evidences, Maintaining Chain of Custody, Maintaining Information Flow, Addressing Safety Issues and Maintaining an Accurate Case Management. The field of forensics in which this model can be applied is not also clear. From the descriptions provided in their paper, it appears that the IDFPM's focus is on the field of incident response. If the model's intended usage were aimed at the law enforcement environment, then it would need additional Processes such as Securing and Evaluating the Crime Scene based on the ACPO (2012) and the approach taken by the thesis author in Montasari (2016, b and c). However, as it stands, the IDFPM does not provide details for such a Process.

In relation to the Beebe and Clark's criteria, the IDFPM meets only Requirements 2 and 4 as the authors have been able to simplify the complex investigative process. The model does not have scientific rigor due to its lack of flawed classification of Sub-Processes as a Processes (Requirement 1). The model also does not contain sufficient level of details, nor does it have the flexibility to incorporate the needed granularity (Requirement 3). In addition, the IDFPM has not defined standard assumptions, concepts and values (Requirement 4). The Beebe and Clark score given to this model is 2/4.

Using the Carrier and Spafford, the IDFPM meets only Requirements 1 and 3. The model has basis in physical crime scene theory (Requirement 1), and it is not dependent on a specific technology (Requirement 3). However, the IDFPM is not practical due to the lack of precise ordering of its Sub-Phases as well as essential investigative Principles (Requirement 2), and the model is not specific enough to facilitate technology development because of inconsistencies in its data flow (Requirement 4).

Moreover, the IDFPM is not generic as it appears that it only focuses on the field of incident response (Requirement 5). The Carrier and Spafford score given to the IDFPM is 2/5.

In terms of the Daubert Test, the IDFPM only meets Requirement 2 as the model has been peer reviewed and published. However, it has not been tested by the experts in the field (Requirement 1); therefore, its potential error rate is unknown (Requirement 3). There is also no standard associated with the IDFPM (Requirement 4). Also, there is no evidence suggesting that the IDFPM has been widely accepted in the field of digital forensic community (Requirement 5). The Daubert Test score given to this model is 1/5.

2.7.20 Adams et al's ADAM

Adams et al. (2014) criticised the previous models for focusing on one specific area of digital forensic practice, arguing that such approach has hindered the establishment of "generally-accepted standards" for a fundamental digital forensic activity – the acquisition of digital evidence. As a result, Adams et al. (2014) go on to propose a three-step model, The Advanced Data Acquisition Process Model (ADAM) (originally presented in Adams (2012)), so that it would be applicable to different fields of digital forensics.

The ADAM focuses only on the data acquisition aspect and consists of three stages including: Initial Planning, the Onsite Plan and Acquisition. The first stage of the model, Initial Planning, involves high-level consideration to be undertaken prior to the actual Data Acquisition Process. Stage 2 requires investigators to attend the scene of the incident to determine the location, size and format of the devices containing the digital data, and to create the Acquisition Plan. Stage 3 involves the performance of the actual digital Data Acquisition Process on a digital device.

Adams et al. (2014) state that the lack of "generally-accepted standards" has hindered the establishment of a fundamental digital forensic activity – the "acquisition of digital evidence", a view supported also by other researchers. For example, Cohen (2012) states that the entire field of digital forensic still lacks consensus on the fundamental

areas. Therefore, the lack of generally accepted standards not only pertains to the Acquisition Stage, but also relates to the entire investigative process, a view supported by many other researchers as discussed in the Introduction Chapter (Montasari et al., 2015; Kohn et al., 2013; Agarwal et al., 2011; Garfinkel et al., 2009; Carlton and Worthley, 2009).

A detailed and close inspection of the Adams' study, presented first in Adams (2012) and subsequently in Adams et al. (2014), has revealed many advantages in terms of both Adams' background research into the previous DFIPMs, as well as the design and development of the ADAM, itself. Adams full research presented in Adams (2012) is probably the most comprehensive study of the previous DFIPMs presented to date.

Unlike many other researchers who have often taken a cursory approach in relation to DFIPMs, Adams (2012) has delved into the study of previous DFIPMs prior to the design and development of their Advanced Data Acquisition Process Model. Adams (2012) has studied the previous literature in order to identify the essential components for the three stages of their model, in particular that of the Initial Planning stage.

The ADAM has provided a detailed discussion concerning its Initial Planning Stage which is a commendable approach (some components of this stage are used in the new model). Unlike the previous models which always take a cursory approach in relation to discussing the investigation planning, Adams (2012) has covered various important issues in detail such as those associated with the legal authorisation of digital investigation, timing constraint, data constraint and issues concerning logistics.

Another benefit of the ADAM lies in its usage of the Unified Modeling Language to present the model in a formal manner. The Onsite Plan of the ADAM equally is detailed and provides useful tips with regards to activities in relation to conducting "Preliminary Survey" at the scene of the incident. Furthermore, unlike many of the authors of the previous models who have not tested their models, Adams has subjected the ADAM to two sets of evaluation process, including cases studies and also independent evaluation of his model by experts.

Moreover, in many cases, often the authors of the previous models appear to have neglected the essential Overriding Principles of Digital Forensic Practice. However, Adams (2012), relying upon the ACPO guidelines as well as other research papers, has provided an operation guide which is intended to accompany the ADAM enabling investigators to conduct digital forensic investigations in a forensically sound manner.

Although ADAM has many advantages, it is also open to some criticism (similar to any other DFIPM). One of the shortcomings of this model is due to the fact that it does not cover the entire digital forensic investigative process as it has focused only on three stages of digital investigation, namely planning, onsite plan and data acquisition. Thus, certain essential stages of the investigative process such as Incident Detection, First Response, Examination, Analysis, Interpretation, Reporting, Presentation and Investigation Closure have not been covered. In fact, Adams (2012), himself, calls for other researchers to expand upon the ADAM to cover other stages of digital investigative process such as analysis and presentation.

Within the Data Acquisition stage of the ADAM, there are some essential steps that have not been included. For instance, although Adams (2012) has provided the option of "Returning" or "Storing" the evidence, they have not provided any components for the 'destruction' or 'cleansing' of the evidence. In certain circumstances where the digital device has contained sensitive material, the law will often require the destruction of the device once the investigation has been finalised.

Moreover, Adams has undertaken a high-level approach towards the Acquisition stage of the model, arguing that this should be "the role of the digital forensic practitioner to determine the most appropriate activities associated with data acquisition". Such an approach would leave DFIs to select components for the Acquisition stage themselves which might result in inconsistencies. As a result, this will undermine the notion of a "generally-accepted model" which requires some sorts of formalisation to acquire such a status. Being labelled as a Digital Forensic Investigator or Practitioner does not necessarily denote that they have adequate 'scientific' skills to define components for a process model which is the role of a 'theorist'.

One of the reasons why DFIPMs have not been formalised is due to the fact that these have often been developed by practitioners based on their own personal experience as stated by Valjarevic and Venter (2015) rather than scientists. Thus, DFIs should only be required to have adequate 'practical' training, skills and experience to deal with the practical aspect of investigations without being expected to have 'scientific' knowledge of the theory behind the model. Thus, the approach taken by Adams et al. (2014) in this regard might reduce the practicality of the model.

In line with Venter (2006) and Beebe and Clark (2005), a practical model is that which can provide the investigators with a step-by-step guide without limiting their flexibility when conducting investigations. Moreover, such a high-level approach taken by Adams (2012) towards the main stage of his model (Acquisition) appears to be contradictory to their criticism of Khatir et al's (2008) model, where the former author criticises the model proposed by the latter, in Adams (2012), stating,

> *However, although the key factors of an investigation are identified in a unique format the high-level approach is not of great benefit to the investigator as a lot of detail is missing thus limiting the practical aspect of this model as well as the ability to design technology to assist the practitioner.*
> (Adams, 2012)

Such a criticism appears to be invalid considering the fact that Adams (2012), himself, has adopted the same approach as that of Khatir et al. (2008). However, Adams goes on to explain why such approach has been adopted. The author states,

> *Each organisation undertaking the acquisition of digital evidence should have developed their own procedures to supplement those of the ACPO and ISO Guidelines but inevitably it is down to the practitioner to decide how these guidelines are to be applied in a particular set of circumstances.*

Adams et al. (2014) have also stated that the outcome of employing their model is a clear process description that can be explained in courts that will describe the activities in relation to the acquired digital data. However, courts would need to consider the entire investigative process that the investigators have followed in order to be able to determine the reliability of digital evidence presented to them. As a result, courts are very likely to require a model that has captured the 'entire' investigative process, as opposed to a model that has covered only a few stages of the investigative process.

In other words, courts do not reach their decisions on the basis of a few stages in a digital investigation as implied by Adams (2012). There are other essential stages of the investigation such as digital evidence Examination, Analysis and Interpretation, etc. that will need to be described to the courts. The decision to prove or refute the reliability of digital evidence is made only after the judge and jury have taken into consideration a collective process of digital evidence 'Acquisition', 'Storage', 'Handling or Chain of Custody', 'Examination', 'Analysis', 'Interpretation', 'Event Reconstruction' and 'Documentation'.

The Acquisition stage of the ADAM is also missing some essential activities pertaining to those of the 'Onsite Triage' as suggested by Montasari (2016, b), Parsonage (2009) and Rogers et al. (2006). In certain circumstances, where the case involves investigation into missing children or abduction, an Onsite Triage[22] will be required with the purpose of acquiring investigative leads as swiftly as possible within minutes as opposed to days or weeks. The ADAM's Acquisition stage, however, has not provided any components to accommodate for activities associated with the Onsite Triage. Finally, despite few shortcomings of the model, Adams (2012) has been able to take a scientific approach in developing the ADAM. Adams (2012) rigorous approach in conducting his study is another reason why the ADAM stands out from all the previous DFIPMs.

In relation to the Beebe and Clark, the ADAM meets Requirements 2 and 4 fully and also Requirement 1 partially. Although the model is not comprehensive as it does not

[22] This will refer to the prioritisation of digital devices at the crime scene suspected of containing potential digital evidence based on their potential evidential value and then swift examination and analysis of the prioritised devices.

cover the entire investigative process, it has achieved both rigor and relevance due to its detailed approach towards the Initial Planning stage (Requirement 1). Moreover, the authors have simplified the complex investigative process through the use of UML Diagrams (Requirement 2). However, the ADAM does not have granularity throughout all the three stages (Requirement 3). Adams et al. (2014), however, have defined important concepts and practices such as those of some investigative principles including consideration of Documentation and Chain of Custody (Requirement 4). The Beebe and Clark score given to this model is 2.5/4.

Using the Carrier and Spafford criteria, the ADAM has met Requirements 1, 3 and 4. The model has basis in existing theory for physical crime investigations (Requirement 1), and it is not limited to a specific technology (Requirement 3). Although the model is not detailed in terms of its Onsite Plan and Acquisition stages, it has provided sufficient details for its Initial Planning stage to allow for creation of technical aids (Requirement 4). However, since the model does not cover the entire investigative process, it might not be practical in actual investigations (Requirement 2). Moreover, it is not clear whether or not the model is generic, as it appears to be more relevant to the environment of commerce (Requirement 5). The Carrier and Spafford score given to the ADAM is 3/5.

With regards to the Daubert Test, the ADAM has only met Requirements 1 and 2. The model has been tested by experts in the field (Requirement 1); however, its potential error rate is not fully known due to the low number of experts who have participated in the model's evaluation. The authors, themselves, state that a more diverse set of experts will need to be involved to test the model (Requirement 3). The ADAM has been subjected to peer-review and publication (Requirement 2). However, there is no standard that governs the development of the ADAM with the exception of the ACPO's four principles that Adams (2012) has referred to (Requirement 4). Moreover, there is no evidence suggesting that this model has been widely accepted in the digital forensic community (This might be explained by the fact that the model is still relatively new and has not yet fully reached a wider user community), nor is there any evidence showing that there has been further development of the model since it was published (Requirement 5). The Daubert Test given to this model is 2/5.

2.8 Analysis of Model Review and Assessment

The critical review and assessment of the previous models reveal that as of May 2016, there is no comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonises and extends the previous models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response. The literature review also reveals a lack of scientific consensus in the domain of digital investigative process. Although many researchers have increasingly called for scientific approaches and formal methods, very little progress, if any, has been made. In this regard, the US-CERT organisation states,

> *Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal "scientific" discipline* (US-CERT, 2012).

A summary of the comments derived from the literature review demonstrates the absence of agreement between researchers and digital forensic investigators alike:

- Previous models are not abstract (Reith et al, 2002).
- Previous models are not comprehensive as they do not capture the full scope of an investigation. Instead, they focus only on the processing of evidence (Ciardhuáin, 2004).
- Previous models are not comprehensive and are not generally accepted. They are single-tier, higher order process models that focus on abstract rather than concrete investigative principles (Beebe and Clark, 2005).
- Previous models do not have a pragmatic and practical approach (Rogers et al., 2006).
- Previous models have not established a clear, step-by-step guide to what steps should be followed in a forensic process (Kohn et al., 2006).
- Previous models have no flexibility (Khatir et al., 2008).
- Previous models are not consistent and systematic frameworks for digital forensic investigation process (Agarwal et al., 2011).

- Previous models are not formal as different authors have adopted their own investigative methods based on their own personal experience (Kohn et al., 2013; Valjarevic and Venter, 2015).
- Previous models have mainly focused on one area of digital forensics and neglect the other environments (Adams et al., 2014).

The following provides a summary of the results of the analysis of the model assessments:

- No model could be considered comprehensive as the majority of the models captured only parts of the investigative process (very often the middle part).
- Although some authors have attempted to develop a generic model appropriate for the different fields of digital forensics, some have instead focused on one particular domain such as that pertaining to incident response.
- No model could be regarded formal as they all had differing focus and approaches.
- The previous models had a heavy focus on single-layer, higher-order process lacking the sufficient detail needed to assist the investigators.
- Despite the fact that the previous models have been peer-reviewed and published, none has been subjected to any form of testing with the exception of EMCI, CFFTPM and ADAM.
- No model included or referenced any standards against which an error rate could be calculated (Adams, 2012), nor was any model identified that has been widely accepted.
- There has been very little consensus in relation to the definition of digital forensic process.

Table 1 provides a comparative summary of the previous DFIPMs that were reviewed and assessed in this chapter. The columns in the Table list the models themselves, while the Table's rows indicate the different components of those models as identified and discussed. Also, those cells marked with a "✔" sign indicate the existence of a particular component within a specific model.

Table 1. The comparative summary of the existing DFIPMs

The Comparative Summary of the Existing Digital Forensic Investigation Process Models (DFIPMs)																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Readiness				✔	✔		✔	✔				✔							✔	
Deployment				✔			✔	✔											✔	
Policy/ Procedure										✔		✔							✔	
Operational Readiness				✔			✔					✔							✔	
Infrastructure Readiness				✔			✔					✔							✔	
Incident Detection (Awareness)			✔	✔	✔	✔						✔						✔	✔	
Report Incident (Notification)				✔	✔	✔		✔		✔				✔					✔	
Assess Incident.								✔					✔						✔	
Confirm Incident.				✔	✔		✔						✔	✔					✔	
Authorisation				✔	✔	✔	✔			✔		✔	✔	✔			✔	✔	✔	✔
Incident Response				✔			✔	✔	✔			✔						✔		
Planning (Approach Strategy)			✔			✔		✔		✔	✔	✔	✔	✔			✔	✔	✔	✔
Understand Task Requirements																				✔
Determine Overall Picture																				✔
Determine Required Outcomes																				✔
Determine Parameters																				✔
Consider Physical Constraint																				✔
Consider Timing Constraint																				✔
Consider Data Constraint																				✔
Plan Logistics																				✔
Create Outline Plan																	✔			✔
Preparation			✔					✔		✔							✔	✔		
Attend Site											✔						✔			✔
Securing the Scene			✔					✔									✔			
Address Safety Issues																	✔			✔
Communication Shielding																	✔			
Triage											✔									
Examine User Usage Profiles											✔									
Examine Chronology Timeline											✔									
Examine Browsing Activities									✔		✔									
Case Specifics											✔									
Carry Out Preliminary Survey																				✔
Documentation of Scene				✔		✔		✔									✔	✔		✔
Update Outline Plan																	✔			✔
Search				✔	✔	✔	✔	✔		✔							✔		✔	
Survey				✔	✔		✔	✔									✔			
Identification	✔					✔		✔	✔	✔					✔		✔	✔		
Preservation	✔		✔	✔	✔		✔	✔							✔	✔	✔		✔	
Collection	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	✔
Volatile Evidence Collection									✔			✔					✔			
To Be Continued …																				

The Comparative Summary of the Existing Digital Forensic Investigation Process Models (DFIPMs)																				
Existing DFIPMs	Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
Non-Volatile Evidence Collection									✔			✔								
Authenticate																			✔	
Seizure								✔											✔	✔
Package																	✔			✔
Transport						✔				✔					✔		✔	✔	✔	✔
Storage						✔				✔					✔		✔	✔	✔	✔
Examination	✔		✔	✔		✔		✔	✔	✔			✔		✔		✔		✔	
Harvest								✔				✔							✔	
Reduce								✔				✔							✔	
Identify				✔															✔	
Classify																			✔	
Organise												✔							✔	
Compare																			✔	
Analysis	✔		✔	✔				✔	✔	✔			✔		✔	✔	✔	✔	✔	
Attribute															✔				✔	
Evaluate																			✔	
Hypothesis						✔													✔	
Interpretation															✔				✔	
Reconstruction				✔	✔		✔	✔				✔			✔				✔	
Reporting		✔		✔				✔	✔			✔		✔			✔			
Presentation	✔		✔	✔	✔	✔	✔	✔		✔			✔		✔	✔	✔	✔	✔	
Proof / Defence						✔		✔		✔										
Decision	✔							✔											✔	
Review				✔	✔		✔	✔									✔		✔	
Dissemination						✔		✔											✔	
Returning Evidence			✔					✔					✔							✔
Digital Crime Scene Investigation				✔	✔		✔	✔												
Physical Crime Scene Investigation				✔	✔		✔											✔	✔	
Documentation				✔	✔	✔	✔	✔					✔					✔	✔	✔
Preserving Chain of Custody						✔	✔					✔								✔
Preserving Digital Evidence						✔		✔										✔		
Information Flow						✔												✔		
Case Management						✔							✔							
End of the Table																				

As shown in the next table (Table 2), assessing the previous models against the Beebe and Clark (2005) criteria reveals that there are five models that meet three of the four criteria, while six and five models fulfil two and one out of the four criteria respectively. There are also three models that meet no criteria, while there is one model to which the assessment criteria are not applicable. Similarly, comparing the previous models

against the Carrier and Spafford (2003) criteria reveals that there is one model that fulfils all the five criteria, while there are four other models that meet four of the criteria. There are also four, seven and three models that meet three, two and one out of the five criteria respectively, while there is one model to which the assessment criteria are not applicable. In relation to the Daubert Test, there are two models that fulfil four and three of the five criteria respectively, while three models meet two of the criteria. There are also twelve and two models that meet one and no criteria respectively, while there is one model to which the assessment criteria are not applicable.

Table 2. Scores obtained by the previous models based on the three assessment criteria

Models	Scores		
	Beebe and Clark	Carrier and Spafford	Daubert Test
A Framework for Digital Forensic Science (Palmer, 2001)	2	2	1
Electronic Crime Scene Investigation: A Guide for First Responders (Ashcroft, 2001)	1	2	0
Abstract Digital Forensic Model (Reith et al., 2002)	2	4	1
Integrated Digital Investigation Process (Carrier and Spafford, 2003)	3	4	2
Digital Crime Scene Analysis (Rogers, 2004)	3	4	2
Enhanced Digital Investigation Process Model (Baryamureeba and Tushabe, 2004)	0	1	1
An Extended Model of Cybercrime Investigation (Ciardhuáin, 2004)	3	5	3
Hierarchical, Objectives Based Framework for the Digital Investigation Process (Beebe and Clark, 2005)	3	3	1
Four Step Forensic Process (Kent et al., 2006)	2	3	0
Computer Forensics Field Triage Process Model (Rogers et al, 2006)	3	4	4
Framework for a Digital Forensic Investigation (Kohn et al., 2006)	2	3	1
A Common Process Model for Incident Response and Computer Forensics (Freiling and Schwittay, 2007)	0	2	1
Two Dimensional Evidence Reliability Amplification Process Model (Khatir et al., 2008)	1	1	1
Mapping Process of Digital Forensic Investigation Framework (Selamat et al., 2008)	0	1	1
Digital Forensic Process Model (Cohen, 2009)	2	2	1
Generic Computer Forensics Investigation Model (Yusoff et al., 2011)	N/A	N/A	N/A
Systematic Digital Forensic Investigation Model (Agarwal et al., 2011)	1	2	1
Harmonised Digital Forensic Investigation Process Model (Valjarevic and Venter, 2012)	1	2	1
Integrated Digital Forensic Process Model (Kohn et al., 2013)	2	2	1
The Advanced Data Acquisition Process Model (Adams et al., 2014)	2	3	2

Analysing the results of the Beebe and Clark (2005), Carrier and Spafford (2003) and the Daubert Test criteria applied to each of the models has identified those that include the components suggested by the three aforementioned criteria as necessary for a DFIPM. In total, there are eight models that have been selected for their possible contributions to the CDFIPM based on their high scores achieved in relation to meeting the three sets of the assessment criteria. The next section provides the specific contributions of these models that will constitute the basic structure of the CDFIPM.

2.9 Identifying Key Contributions

The key contributions that have been identified for each of the models selected through the Beebe and Clark (2005), Carrier and Spafford (2003) and Daubert Test criteria are summarised as follow:

Reith et al. (2002) – ADFM

- Introduced the concept that common steps from the previous DFIPMs[23] can be abstractly defined to develop a model that is technology-independent.

- Identified general methods that judicial members can employ to relate technology to non-technical observers.

Carrier and Spafford (2003) – IDIP

- Promoted the concept that a model should be based on existing theory for physical crime investigations.

- Identified the need for a model to be practical and follow the same steps that an actual investigation would take.

- Highlighted the need that a model should be general in relation to technology and must not be limited to current tools.

- Identified the need that a model must be generic and apply to law enforcement investigations, corporate investigations, and incident response.

[23] This refers to using the key aspects of the previous DFIPMs. Adams (2012) also uses this contribution.

Ciardhuáin (2004) – EMCI

- Introduced the concept of merging the previously proposed models and extending them by addressing certain activities not incorporated into the previous models.

- Emphasized the need for a comprehensive model that captures the entire investigative process.

- Introduced the concept that a DFIPM should be tested by its intended user community as well as being compared with previous models.

- Introduced the concept of "Information Flow".

- Identified the need for both internal and external authorisations.

Rogers (2004) – DCSA

- Highlighted the need for the Chain of Custody consideration.

- Built upon the relationships between digital and physical investigations as first proposed by Carrier and Spafford (2003).

Beebe and Clark (2005) – HOBFDIP

- Emphasized granularity in a model with the inclusion of additional layers of details as opposed to a single-tier, higher order process model.

- Emphasized the need for a comprehensive, generally accepted process model.

- Highlighted that a model should simplify complex processes to facilitate understanding of the underlying structure.

- Underlined the need for digital investigation Principles and that they should apply to the entire investigative process and should not therefore be "cordoned off" as distinct, discrete Phases or steps.

Rogers (2006) – CFFTPM

- Promoted a practical and pragmatic approach matching the steps taken in actual investigations.

- Introduced activities for performing Onsite Triage in relation to Identification, Analysis and Interpretation of digital evidence in a short time frame while adhering to commonly held digital forensic Principles.

Kohn et al. (2006) – FDFI

- Emphasised the need for a clear, step-by-step guide for the acquisition of evidence appropriate for presentation in courts.

- Promoted the idea that a DFIPM must be systematic to produce forensically sound evidence.

- Emphasised considerations for standards, policies, procedures, training and legal advice in organisations to assist them in investigations.

Adams et al. (2014) – ADAM

- Provided a detailed list of activities in relation to Initial Planning that should be carried out onsite.

- Emphasised the need to apply a DFIPM to different case studies.

- Emphasised the need for the use of UML Activity Diagrams within a DFIPM to define process flows in a formal manner.

2.10 Identifying Necessary Elements for the CDFIPM

By synthesizing the key contributions as well as considering the reviewed models collectively, the necessary elements for the CDFIPM are now summarised and categorised into seventeen stages:

1. Readiness stage, where organisations should take certain pro-active steps in advance of a potential digital crime to increase the chances of digital evidence being available, with the aim of deterring, detecting, responding, investigating and prosecuting computer crimes.

2. Incident Detection stage, containing the activities associated with the incident detection and its reporting.

3. First Response stage, including activities related to initial, pre-investigation response to a suspected digital crime.

4. Planning stage, where a detailed plan of action needs to be drawn in relation to the investigation and investigation logistics.

5. Preparation stage, involving the implementation of the activities detailed in the Planning stage.

6. Secure and Evaluate the Crime Scene stage, dealing with the suspect and the crime scene where pre-data acquisition activities need to be undertaken such as creating an outline plan and securing the crime scene.

7. Identification stage, where investigators need to identify the items that might contain potential digital evidence.

8. Acquisition and Collection stage, containing the activities associated with the actual data acquisition, duplication and verification process, as well as those associated with the transportation and storage of digital device.

9. Examination stage, where data representing potential digital evidence needs to be accessed, identified and extracted using a large number of techniques.

10. Analysis stage, containing activities to enable investigators to reconstruct fragments of data based on their significance and determine a possible root cause of the incident.

11. Interpretation stage, where scientifically proven methods need to be used to explain facts discovered during the Analysis stage within the context of investigation.

12. Event Reconstruction stage, in which investigators also need to use scientifically proven methods to prove or refute theories based also on the Analysis stage.

13. Reporting stage, requiring the investigators to compile and write a concise report.

14. Presentation stage, where the output from the Reporting stage in the form of a well-written report must be presented to the relevant audience such as courts of law.

15. Investigation Closure stage, where activities related to closing the investigation formally take place such as returning the evidence, reviewing the entire investigation and disseminating the investigation results, etc.

16. Future Readiness stage, containing activities to assist both the investigating and victim organisations to take certain steps to be prepared for the future incidents.

17. Overriding Principles group, containing a set of investigative Principles that investigators will need to apply concurrently throughout other stages of the investigative process.

18. The CDFIPM will be described through a formal definition employing the UML as first suggested by Bogan and Dampier (2005) and supported by Adams (2012), Ruan and Huebner (2009) and Kohn et al. (2008).

2.11 Summary of the Chapter

This chapter critically reviewed the existing body of knowledge associated with the domain of digital forensics. First, it provided a general overview of the digital forensic investigations followed by a detailed review of the field of digital evidence and how its admissibility is governed within the U.K. and the U.S. jurisdictions. Next, a critical review of the standards associated with the digital investigative process was provided. The chapter then introduced different assessment criteria against which previous models were to be assessed. The chapter continued to cover the process for identifying those models that could contribute to the design and development of the proposed model by assessing each previous model against the assessment criteria.

Following the identification of the prevailing models, their key contributions were determined based on the assessment criteria. Finally, in this chapter, the necessary components for the proposed model were identified from the key contributions of the prevailing models, as well as from all the reviewed models collectively. It is contended that the assessment process of the previous DFIPMs is the most comprehensive evaluation that has been conducted so far, and is the first to evaluate each model against three different sets of assessment criteria.

Chapter 3: Design and Development

3.1 Introduction

This chapter follows the Design and Development stage of the Peffers et al's (2006) DSRP model that has been used to carry out this research. A critical review and assessment of the existing models were carried out in Chapter 2 to address the following three research questions:

1. What are the essential components necessary in a comprehensive model that is formal, generic and forensically sound for the entire digital forensic process?

2. Once the components of such a comprehensive model that is formal, generic and forensically sound are determined, how can they be integrated into a working model?

3. What is the most appropriate method to describe, present and use the model for the entire digital forensic process?

Having acquired the information concerning the above three research questions, this chapter now continues to implement the design and development of the new model, the CDFIPM.

3.2 The Central Requirements of the CDFIPM

All the prominent DFIPMs presented to date were critically reviewed and assessed in Chapter 2 to identify necessary components for the CDFIPM. The rationale in doing so was multifaceted. Firstly, it was intended to leverage the benefits of the previously proposed models. Secondly, it was intended to bring other experts' knowledge and experience into the CDFIPM to create synergy between different points of view. From this critical analysis, various drawbacks concerning the previous DFIPMs were identified as follows:

1. The DFIPMs are not comprehensive in that they do not cover the entire digital investigative process. They have tended to focus on the middle part of digital forensic process, i.e. the Collection and Examination of digital evidence.

2. The majority of the existing DFIPMs are not generic in that they cannot be applied in both environments of criminal prosecution resulting in a court of law and organisations' breaches of information security. The DFIPMs have often been predominantly created with only one domain of digital forensic in mind.

3. The existing DFIPMs are not formal in that they are inconsistent in terms of differing numbers and types of processes as well as conflicting terminology.

4. The majority of the DFIPMs have not included the activities that are not forensic in nature yet closely related to digital forensic process, such as activities for organizations' readiness, incident response or incident closure.

5. Some DFIPMs confuse the different activities of incident response and digital forensics resulting in improper activities (such as network-biased requirements) with an excessive focus on an environment that is not representative of a generic workspace for digital forensic investigators (Adams, 2012).

6. Models have differing concepts applied to their development (for example, many of the process models are based on physical crime investigation processes).

7. Most of the existing models have not paid attention to the proper order for the activities introduced in these models.

8. The greatest problem associated with the existing models pertains to their lack of adequate level of detail (granularity). These models are overly high-level (single-layer processes) resulting in failure to incorporate sufficient details.

The design and development of the CDFIPM is intended to contribute towards addressing the identified shortcomings associated with the existing DFIPMs in order to accommodate new and emerging technology by achieving the research aim (as outlined in Section 1.4.1). Therefore, the design and development of the CDFIPM will be guided by the following three fundamentals:

- The CDFIPM must be comprehensive.
- The CDFIPM must be formal.
- The CDFIPM must be generic.

In relation to the point 3 above, due to the fact that the CDFIPM is to be a generic model, it cannot be prescriptive with regards to organisational guidelines. However, in line with Adams' (2012) Advanced Data Acquisition Model, the CDFIPM needs:

1. To incorporate the overriding principles derived from the guidelines in ACPO and also ISO/IEC standards;

2. To accommodate organisational policy and practice such as guidelines, signing authorities and other requirements;

3. To accommodate procedures and techniques that can be adapted and expanded upon as new data becomes available; and

4. To include the key contributions from previous researchers.

Moreover, the CDFIPM will be based on an 'objectives-based approach' as opposed to a 'tasks-based approach'. This is due to the fact that a model which is based on a pre-defined check list is counter-productive as it can limit both the practicality of the models as well as the investigators' flexibility. Moreover, a pre-defined check list approach cannot predict different situations due to the uniqueness of each given situation. Thus, in line with Beebe and Clark (2005) and Carrier and Spafford (2003), the uniqueness of each situation requires a non-checklist approach such as that of 'objectives-based approach'. For the purposes of this thesis, objective is defined as something which is intended to be achieved, whereas the task is defined as something

which needs to be done in order to achieve the objective. Therefore, an objectives-based approach as suggested by Beebe and Clark (2005) and Carrier and Spafford (2003) will be adopted when designing and developing the CDFIPM. Determining what steps to take in a particular digital crime investigation can easily be made by the DFIs themselves when the steps are detailed in an objectives-based manner rather than a tasks-based approach.

Prior to describing the CDFIPM in section 3.4, its design elements will be discussed and justified in the next section.

3.3 Fundamentals of the CDFIPM

3.3.1 Fundamentals of the New Model

One of the issues associated with the previous DFIPMs is the lack of standardized terminology within those models (Montasari et al., 2015; Valjarevic and Venter., 2015; Cohen 2011; Ciardhuáin, 2004; Reith et al. 2002). It is not the digital evidence itself that needs to be prevailed in a court of law; the terminology used should also be rigorous and widely accepted within the digital forensic community (Kohn et al., 2013). To address this issue, the terminology within the previous DFIPMs were studied to identify similar meanings in the terminology and extract the most agreed-upon terminology from those DFIPMs for inclusion in the CDFIPM. It is argued that the CDFIPM provides a uniform terminology after having considered and purified the terminology used in the previous DFIPMs.

3.3.2 Design of the CDFIPM Formal Representation

The existing DFIPMs have often been presented in an informal way. For instance, most models are presented in text, with some aided only by tables (Ruan and Huebner, 2009). This has also contributed to a lack of formalisation in relation to the DFIPMs which, according to Ruan and Huebner (2009), could lead to "ambiguous semantics of the model if sufficient level of detail is not captured". Also, in this regard, Kohn et al. (2008) state,

Most of the modelling representations for forensic investigations found in the current literature are made in a rather informal and intuitive way. Thus, it is argued that because of the value of a forensic investigation the formal field of forensic investigation can benefit from introducing a formal modelling approach.

Kohn et al. (2008), relying on the supporting arguments presented previously by Bogan and Dampier (2005), suggest the Unified Modelling Language (UML) as an appropriate paradigm for modelling forensic process. Similarly, Ruan and Huebner state, "What is needed is a formal model to specify the methodology used in the digital forensic analysis, which can provide well-defined and straightforward semantics to the digital forensic process (Ruan and Huebner, 2009)." In consonance with Bogan and Dampier (2005) and Kohn et al. (2008), Ruan and Huebner also suggest that the introduction of the Unified Modelling Language (UML) methodology to the digital forensic process provides formalism and a structured approach to digital forensic processes (Ruan and Huebner, 2009). Therefore, based upon these supporting arguments, the UML was considered as an appropriate paradigm to model the entire digital investigative process in a formal manner within the CDFIPM.

Although the UML has been previously applied in few research studies for modelling digital forensic process (Valjarevic and Venter, 2015; Adams, 2012; Kohn et al., 2008), its application has been limited to high-level components without providing any adequate or low-level details. In contrast, this research will develop the use of the UML in digital forensics, which is discussed in the following section.

3.3.2.1 Selected Type of Unified Modelling Language

The UML is a de-facto standard modelling language (Adams, 2012), the primary purpose of which is visualisation (Ruan and Huebner, 2009). It is "intentionally process-independent", making it suitable for modelling "different processes" as well as analysing, designing and implementing artefacts such as models and systems (OMG, 2016). The UML specification defines 14 types of UML Diagrams divided into two main categories including Structural Diagrams and Behavioural Diagrams (OMG, 2016). Structural Modelling captures the static features of a process or a system without

describing its dynamic behaviour. In contrast, the Behavioural Modelling not only describes the interaction in the process or system but also represents its dynamic features.

The type of UML Diagram selected for modelling the entire digital investigative process within the CDFIPM is the UML Activity Diagram under the Behavioural UML category. This research will develop the use of UML in digital forensics by using the UML Activity Diagrams to define process flows of both high-level and low-level components of digital forensic process. Developing the use of UML in digital forensics is therefore another novel contribution of this research to the field of digital forensics. The rationale for selecting the UML Activity Diagram over other types of Behavioural UML Diagrams or Structural UML Diagrams is multifaceted, which is now discussed in the section below.

Firstly, the UML Activity Diagram is designed to deal with all types of flow control within a process. An Activity Diagram not only describes the sequence from one activity to another but also describes the parallel, branched and concurrent flow within a process. Thus, since the flow of activities in the CDFIPM are either sequential, parallel, branched or concurrent, the use of UML Activity Diagrams was considered more appropriate over other Behavioural or Structural UML types. This will enable the thesis author to model the components of the entire digital forensic process and their relationship more effectively and clearly.

Secondly, the use of UML Activity Diagram to model a digital forensic process is suggested by other prominent researchers within the domain of digital forensics. For instance, Ruan and Huebner (2009), Kohn et al. (2008) and Bogan and Dampier (2005) suggest the use of Activity Diagram and Use Case Diagram, both of which belong to the Behavioural UML category, as the preferred choice of UML Diagrams for modelling the digital forensic process. In this regard, Ruan and Huebner (2009) state that Activity Diagram provides "a well-defined and straightforward semantics" to the digital forensic process facilitating the understanding of the process by various parties involved such as legal advisors or judicial personnel. Although the use of both UML "Activity Diagram" and "Use Case Diagram" was suggested by the three aforementioned references for modelling digital forensic process, UML Activity Diagram is still the preferred choice

within this research. This is due to the fact that as Adams (2012) states, the UML Activity Diagram is more appropriate for describing activities within a process model than the Use Case Diagram. Adams (2012) recommends the use of the Activity Diagrams over the Use Case Diagrams on the basis that the latter contributes little benefit to the description of process models. Moreover, Use Case Diagrams would need to be tailored for each environment since the players would not be the same across all environments thereby making the overall model less generic.

Thirdly, it is contended that the ease of understanding that the UML Activity Diagram offers will enable digital forensic investigators to visualise the various aspects of the digital forensic process more clearly. In turn, this will result in the digital investigations being expedited. Last but not the least, regardless of the benefit of adopting a formal approach from a technical perspective, the use of the UML Activity Diagram, being a form of flow chart, is supported in a court environment (Adams, 2012; Kelly, 2010; Dattu, 1998). Judicial personnel such as judges and legal practitioners are accustomed to UML Activity Diagrams. For instance, in some cases flowcharts have been prepared by the judges in order to assist the understanding of processes followed in a digital forensic investigation (Ogloff et al., 2006). Referring to the UML Activity Diagram, Ruan and Huebner (2009) highlight that a graph based model has the advantage of visualising the process requirements, thus making the model more understandable for the various parties involved.

Therefore, since the UML facilitates the modelling and visualisation of various aspects of digital forensic process, this research will draw upon the UML Activity Diagrams in digital forensics to present both high-level and low-level components in the CDFIPM.

3.3.3 Design of the CDFIPM's Overriding Principles

To enable DFIs to conduct forensically sound digital investigations, a set of 'Overriding Principles' are designed and grouped into a class entitled 'Concurrent Processes Class', the creation of which is another novel contribution of this research (in the context of this study, the term 'Class' does not refer to the same term employed in object-oriented programming, in which a class is a template definition of methods and variables in a particular. Instead, the word 'Class' is used throughout this study simply to refer to the

specific category in which the proposed model's Processes are placed). The Concurrent Processes Class are then incorporated into the abstract representation of the CDFIPM as a unique and distinct group of processes or Overriding Principles.

These principles are encompassing procedures, guidelines and methodological approaches that encompass some or all of the fourteen specified processes of the proposed model as well as its phases and sub-phases. Principles as opposed to phases are not distinct and discrete steps in the process. Rather, they are aims and objectives needed to be achieved throughout the process. Examples of these principles include: maintaining a detailed documentation of digital forensic process, preserving chain of custody, obtaining proper authorisation and managing information flow, etc. These Overriding Principles apply concurrently throughout the entirety or parts of the other processes within the CDFIPM. Due to the space constraint imposed by the size of the CDFIPM when presented in its entirety, these Concurrent Processes will only be included in the abstract view of the CDFIPM in Figure 15.

3.3.4 Hierarchical Structure of the CDFIPM

Any model institutionalized through subsequent intellectual discourse and practical use must take into account differing perspectives and approaches, and the soundness of a digital investigation process model is "a function of usability and acceptability" (Beebe and Clark, 2005). In order to acquire usability and acceptability in relation to the CDFIPM, processes, phases, sub-phases, principles and objectives were integrated to formulate a detailed and scientific process model. Processes, Phases and Sub-Phases are obvious; they are individually separate steps in the process which can sometimes be a function of time and are inevitably sequential or sometimes iterative approach. In the CDFIPM, the output of each process becomes an input to the following process as the model is inherently a process model. The processes of the CDFIPM are tied together through the process model flow accompanied by its investigative principles such as information flow and case management. Therefore, all the processes of the CDFIPM are joined by the information flow. Furthermore, in line with Beebe and Clark (2005), the investigative objective on which the investigation is based also unites the processes of the CDFIPM.

The remainder of this sub-section describes the compositional components that will make up the CDFIPM. The terms 'Classes', 'Processes', 'Phases', 'Sub-Phases' and 'Overriding Principles' are used distinctively within the CDFIPM to refer to the different compositional components and their hierarchy within the CDFIPM's structure. This is to contribute towards achieving both the rigor required in a DFIPM (Kohn et al., 2013; Beebe and Clark, 2005; Carrier and Spafford, 2003) and also the formality needed within the DFIPM (Montasari et al., 2015; Valjarevic and Venter, 2015; Adams et al., 2014). The following points, accompanied by a graphical representation in Figure 14, provide further clarification on the meanings and hierarchy of the aforementioned compositional components within the CDFIPM's structure:

- A Class represents the highest level or the first layer of the CDFIPM and is the main group which includes a different number of Processes (see the footnote 17 under the Section 2.6.1 or the first paragraph under the Section 3.3.3 for the meaning of the term 'Class' in the context of this study).

- A Process is the next level down from a Class and represents the second layer of the CDFIPM. Each Process contains a different number of phases. Processes are obvious and individually separate steps; they can sometimes be a function of time and therefore can be sequential or sometimes iterative. The output of a given process will become the input to the following Process.

- A Phase is the next level down from a Process and the third layer of the CDFIPM. Each Phase might contain a different number of Sub-Phases.

- A Sub-Phase is the next level down from a Phase and the lowest level or fourth layer of the CDFIPM.

- Concurrent Class Processes or Overriding Principles contain Action Principles or Processes that are not confined to a single point in time. The Concurrent Processes or Overriding Principles have a wider scope than a single Process and must be applied concurrently throughout the whole or parts of the other Processes in the CDFIPM.

Figure 14 is a graphical representation clarifying the above descriptions of the compositional components of the CDFIPM.

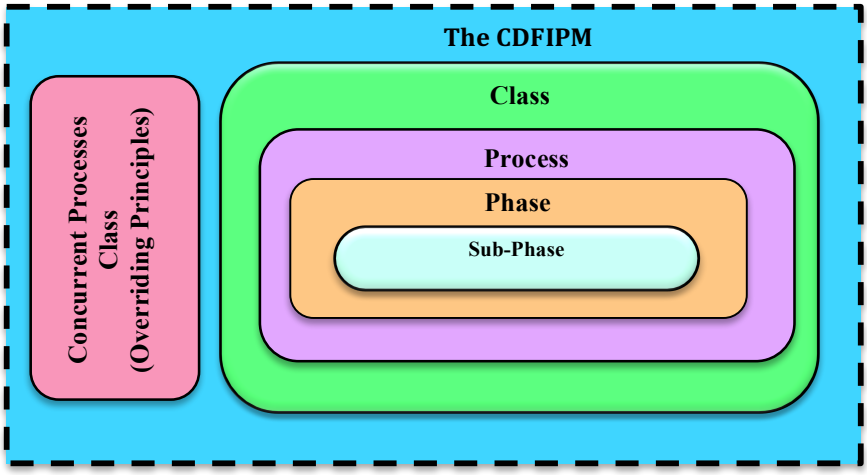


Figure 14. The hierarchical structure of the CDFIPM's components

Having discussed the design elements of the CDFIPM, the following sections describe, justify and incorporate into the proposed model the components that will make up the CDFIPM, building significantly upon the existing DFIPMs.

3.4 The Proposed Model (the CDFIPM)

The CDFIPM has been designed using a top-down approach in order to enable digital forensic investigators to gain a better insight into its compositional components, namely Classes, Processes, Phases, Sub-Phases and Overriding Principles. There are 6 Classes contained within the CDFIPM, each of which contains a different number of Processes. There is a total number of twenty-four Processes included in the six Classes. Apart from the Concurrent Class Processes, which do not provide lower-level details, i.e. Phases and Sub-Phases, the remainder of the Processes provide additional lower layers of details. The CDFIPM will be initially presented in its abstract level, prior to being refined with more details that make up the model's lowest-level structure, that is in its entirety.

Figure 15 represents the first instance of the formal representation of the CDFIPM in its abstract level, containing only the first and second layers of the CDFIPM, namely

Classes and Processes. Following this abstract representation, the CDFIPM will be represented in its entirety in Figures 16-21. Each Process in the CDFIPM is represented by a UML Activity Diagram; the combination of all of the UML Activity Diagrams make up the entire CDFIPM. Due to the space constraint of an A4 sheet, the CDFIPM runs through several pages (when it is in its entirety). Each page is considered to be one figure and depending on the space, each figure might represent more than one Process of the CDFIPM. Therefore, the entire CDFIPM is presented within Figures 16 to 21. After presenting the CDFIPM in its entirety, all the six Classes of the CDFIPM will be subsequently discussed under their associated main headings within Section 3.5 to Section 3.10. Also, the lower-level components of each given Class will be presented and described under the main heading for that particular Class.

Notice that this version of the CDFIPM's formal representation (Figure 15 and Figures 16-21) as well as its Overriding Principles presented in this chapter are prior to their submission to the external reviewers for evaluation and feedback discussed in Chapter 5.

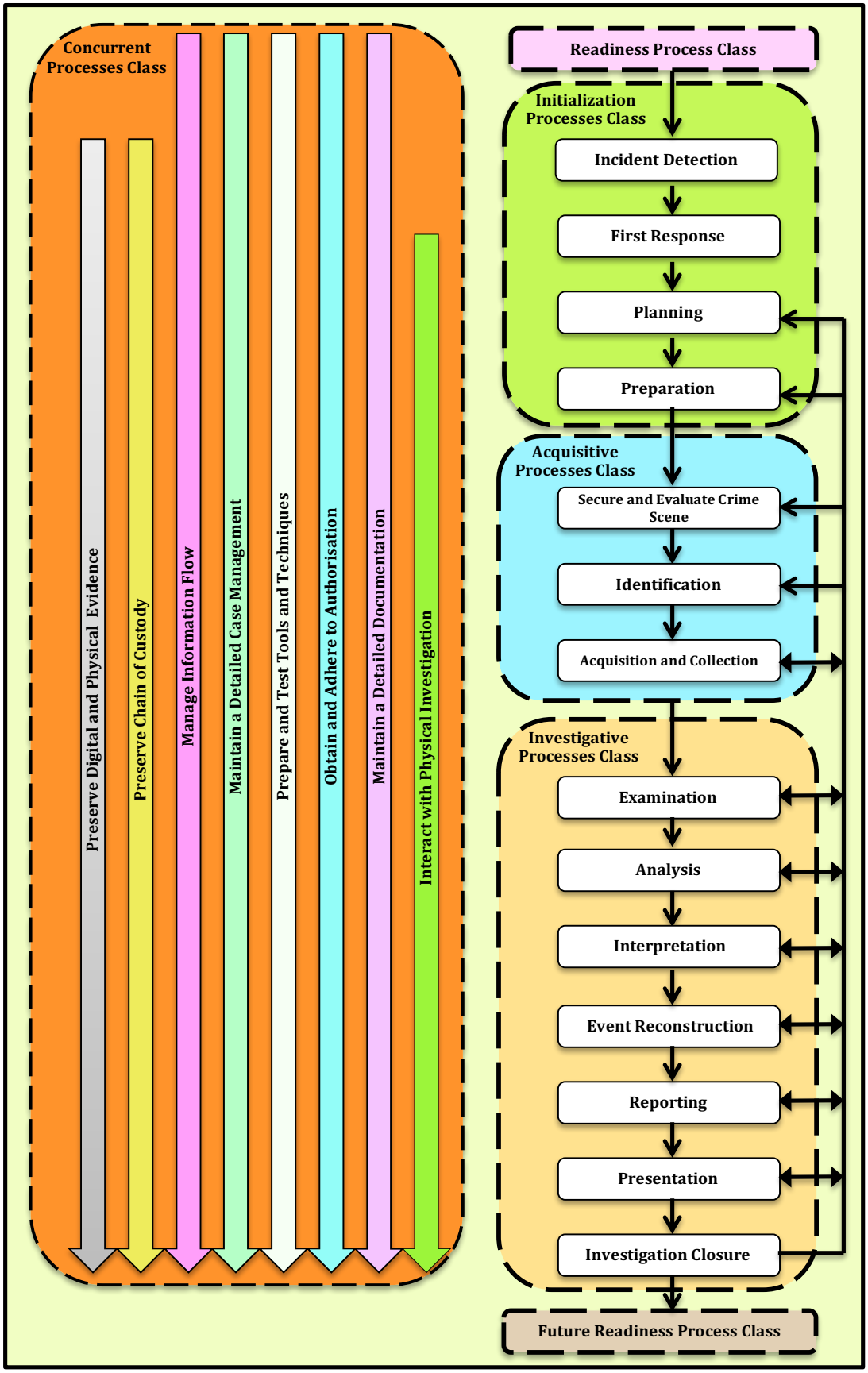


Figure 15. The abstract representation of the CDFIPM

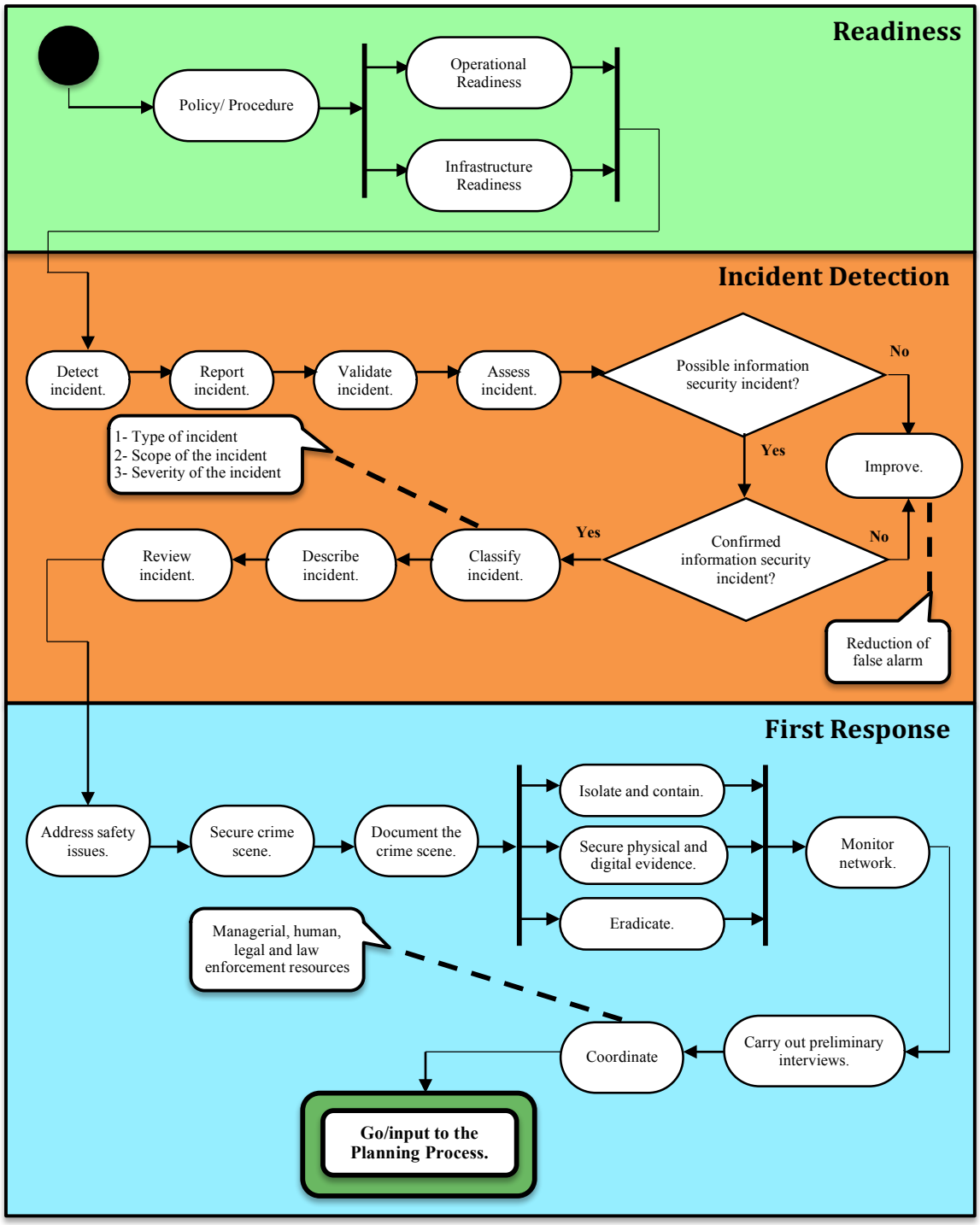


Figure 16. The Readiness, Incident Detection and First Response Processes

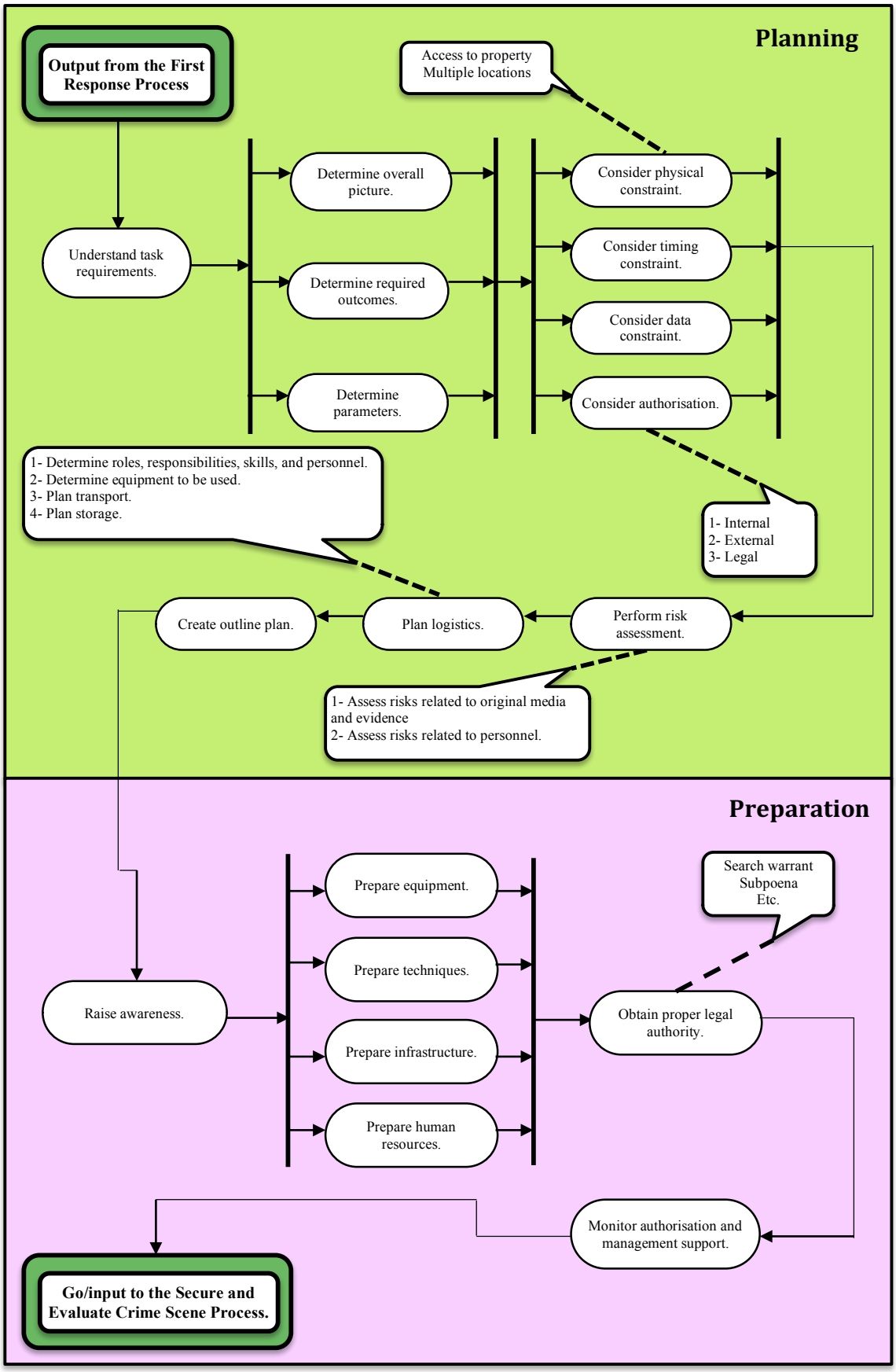


Figure 17. The Planning and Preparation Processes

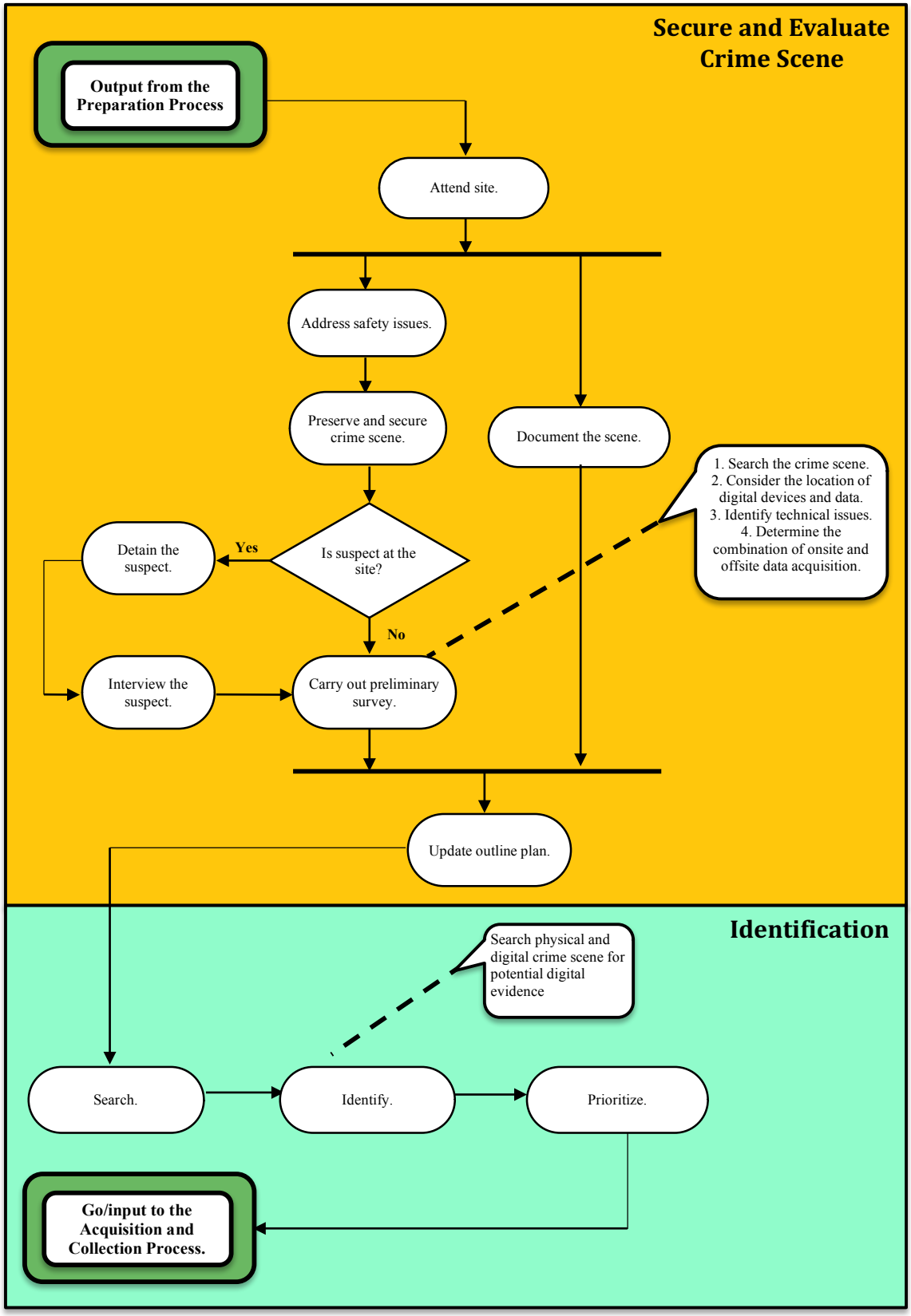


Figure 18. The Secure and Evaluate Crime Scene and Identification Processes

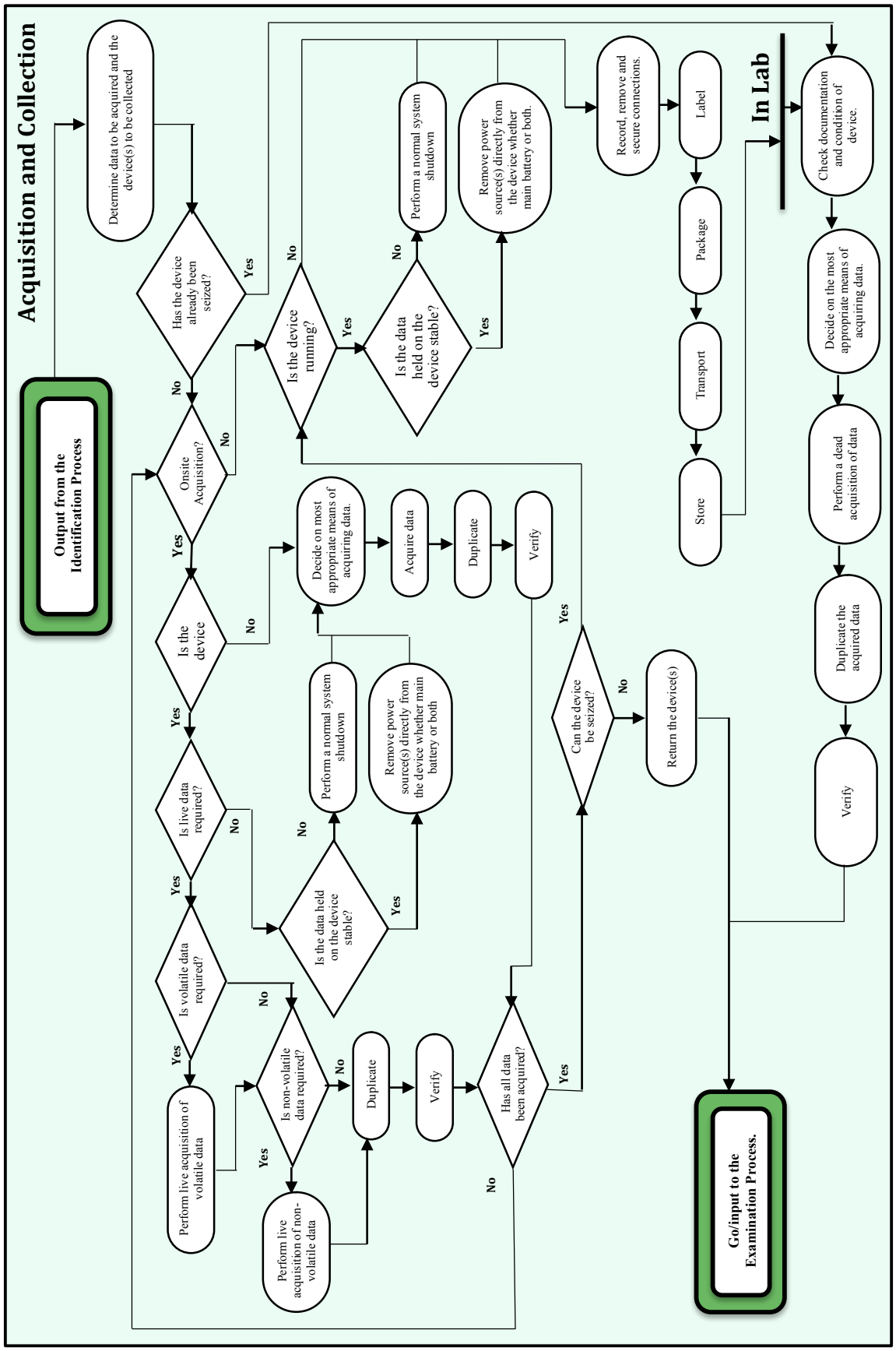


Figure 19. The Acquisition and Collection Process

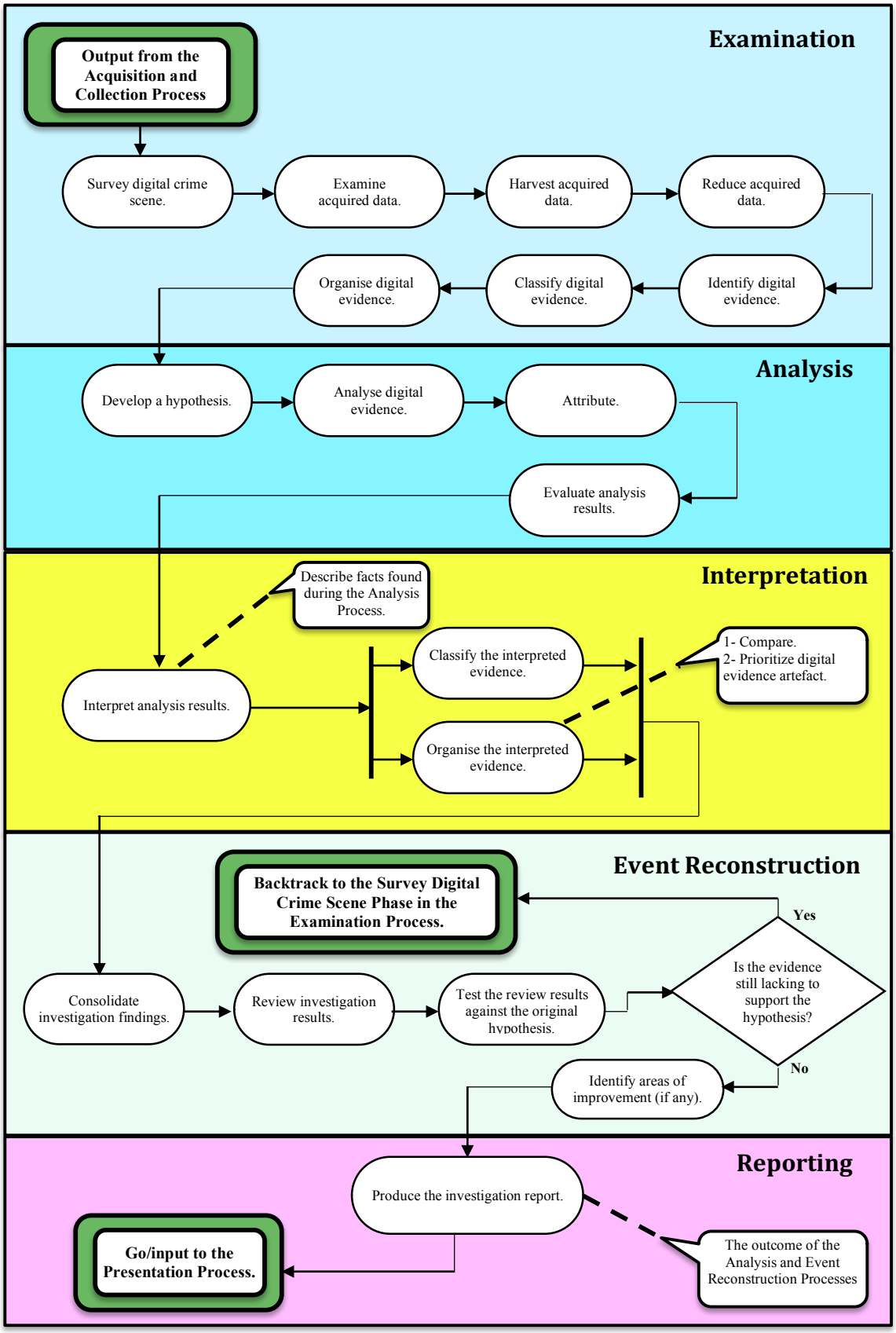


Figure 20. The Examination, Analysis, Interpretation, Event Reconstruction and Reporting Processes

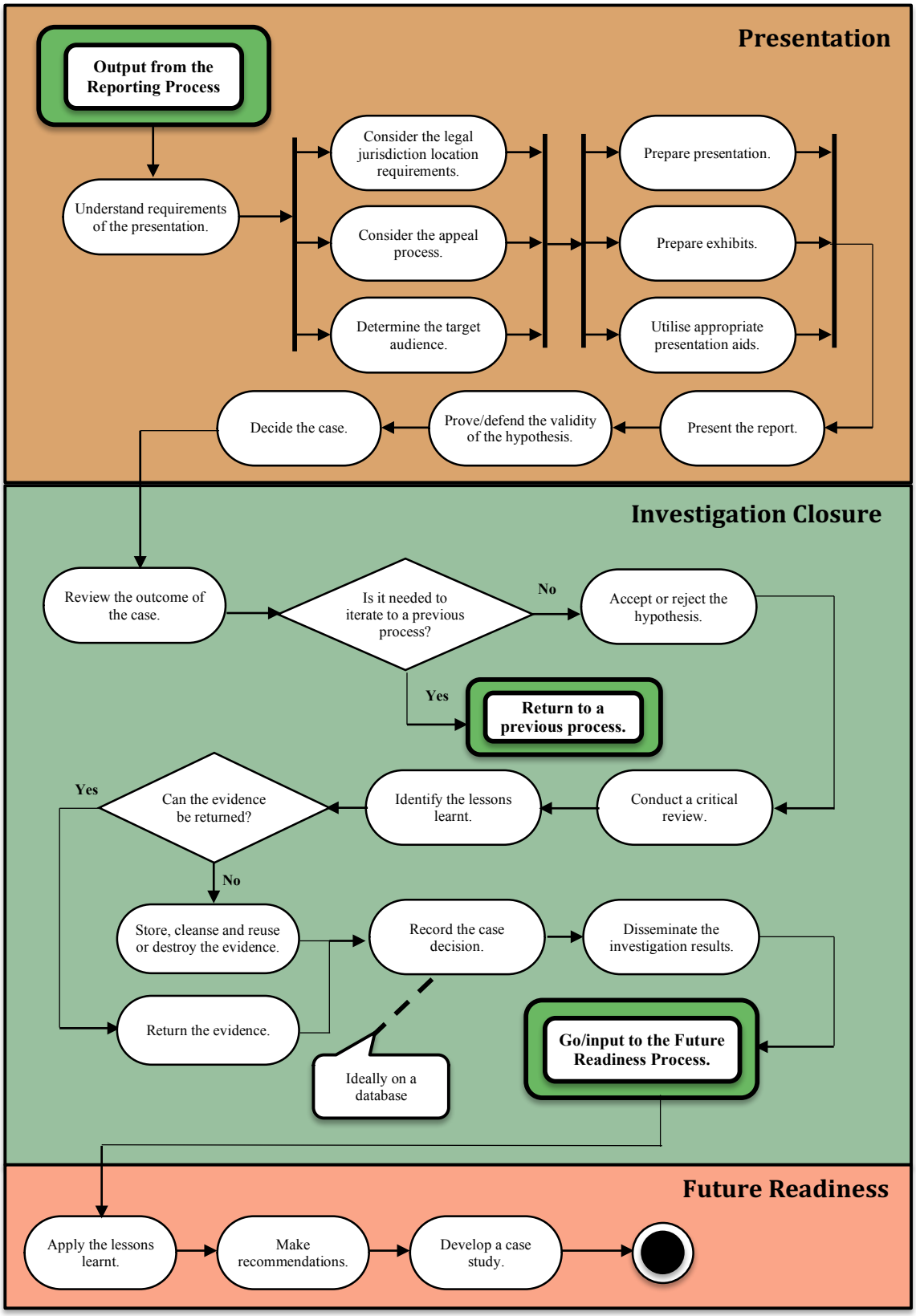


Figure 21. The Presentation, Investigation Closure and Future Readiness Processes

3.5 Readiness Process Class

A digital forensic investigation is often utilised as a post-mortem after a computer crime or an information security breach has occurred. However, careful planning in advance could significantly enhance the quality and availability of digital evidence collected and at the same time, minimise organisational cost and load. This can be materialized through an organisation's Digital Forensic Readiness. Rowlingson (2004) and Tan (2001) define Forensic Readiness as "the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation". This definition is widely accepted and adopted by the digital forensic community. ISO/IEC 27043 builds upon Rowlingson and Tan's definition of Forensic Readiness and suggests that Forensic Readiness is "the ability to maximise the use of the potential digital evidence, minimize the costs of the investigation, minimise the interference with and prevent the interruption of business processes and to preserve or improve the current level of information systems security (ISO/IEC 27043, 2015)".

The two widely accepted aforementioned definitions of Forensic Readiness were used to develop the Phases contained in the Readiness Process of the CDFIPM. The Readiness Process of the CDFIPM is focused on the victim organization, and not the investigator, who is presumably separate from the victim (either functionally, or organizationally). Investigators focus their preparation activities on the Planning Process, technical capability development, training, and evidence preservation handling procedure development. Thus, in the CDFIPM, the Readiness Process Class is used to refer to the pro-active steps that organisations should undertake in advance of a potential digital crime to increase the chances of digital evidence availability with the aim of deterring, detecting, responding, investigating and prosecuting computer crimes. The pro-active steps consist of improved system and staff monitoring, physical and procedural equipment (Rowlingson, 2004), means to preserve data to evidential standards of admissibility (Kohn et al., 2013), processes and procedures in order to ensure that the staff recognise the importance (including the legal significance) of evidence (Casey et al., 2011) and appropriate legal advice and communication with law enforcement (Adams, 2012).

The Readiness Process Class in the CDFIPM contains only one further lower layer, namely Phases, and requires the organisations to focus their efforts on establishing two components including Operational Readiness and Infrastructure Readiness. Figure 22. represents the UML Activity Diagram of the Readiness Process followed by the description of the Phases contained in this Process.

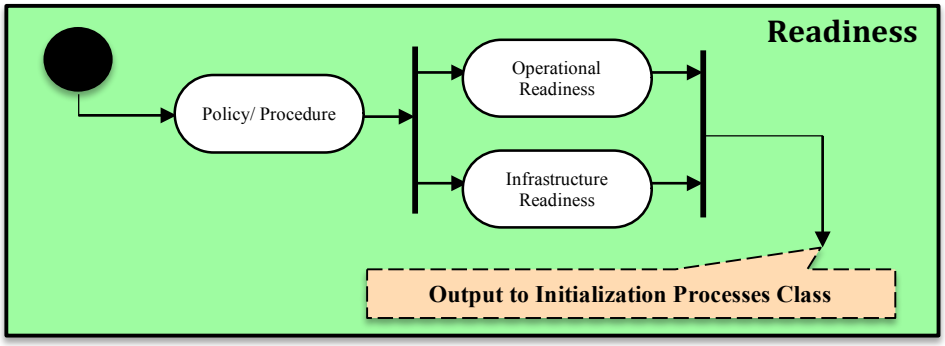


Figure 22. The UML Activity Diagram of the Readiness Processes

3.5.1 Operational Readiness

Under the Operational Readiness, corporates should have a proper initial policy and procedure documents before they can successfully launch an effective digital forensic investigation. The documents and procedures should include a concise description of how the organisation will deal with the digital evidence so that a minimum standard of integrity is maintained when dealing with digital evidence.

3.5.2 Infrastructure Readiness

Infrastructure Readiness, on the other hand, is determined by elements external and internal to the organisation (Kohn et al., 2013). Examples of external elements consist of the legal system, territory legislation, rules of evidence and types of investigation carried out. An example of an internal element is the training of appropriately qualified personnel. The Readiness Process of the CDFIPM is optional to the rest of the digital investigation processes, and are mainly focused on the victim organization and not the investigator who is likely to be separate from the victim organisation either functionally, or organizationally. Moreover, regardless of the field of the digital forensics in which a

digital forensic practitioner operates, the CDFIPM requires investigators to focus their activities on the Planning Process of the CDFIPM, and not the Readiness Process.

3.6 Initialization Processes Class

Initialization Processes Class represents the first layer of the CDFIPM, the aim of which is to deal with the initial stages of a digital investigation. This Class is multi-layered containing three further lower layers including Processes, Phases and Sub-Phase. There are four Processes included in the Initialization Processes Class consisting of Incident Detection, First Response, Planning and Preparation. This section describes these Processes and their associated lower layers, namely Phases and Sub-Phases. Figure 23 represents the UML Activity Diagram of the Initialization Class Processes in their abstract level.

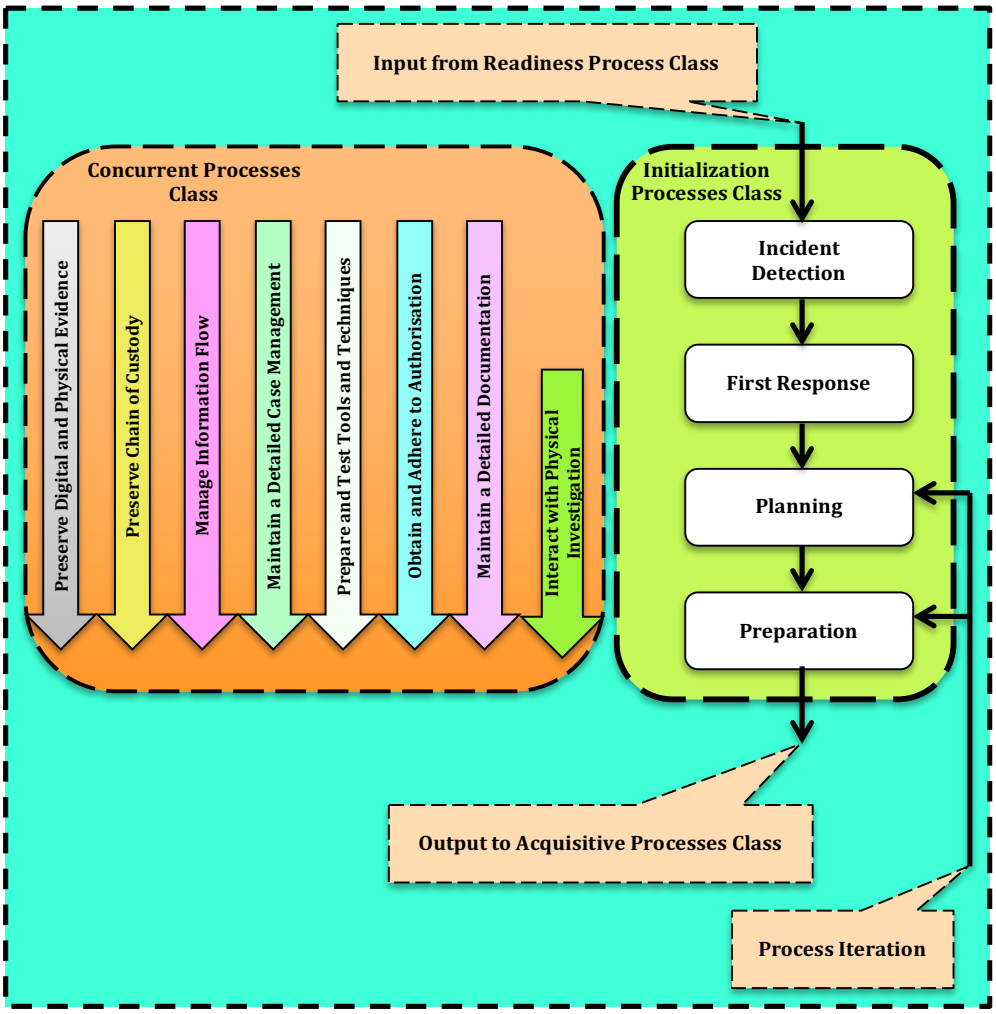


Figure 23. The UML Activity Diagram of Initialization Class Processes in their abstract level

In the following sections the Initialization Processes Class will be broken down to describe its lower-level components, i.e. Processes. In turn, each Process will be further refined in greater details to specify and describe its lower-layer components, i.e. Phases and Sub-Phases.

3.6.1 Incident Detection

In the CDFIPM, the output of the Readiness Process, discussed in the previous section, becomes the input to the Incident Detection Process, which is a multi-layered Process consisting of both Phases and Sub-Phases. The Incident Detection Process is introduced as the first Process of the digital investigation in the CDFIPM denoting that the actual digital investigation starts with this Process. Although authors of few existing models have discussed Incident Detection to some extent, they have often incorrectly suggested Incident Detection as an activity within "Preparation" or "Planning" Phase. In contrast, in the CDFIPM, Incident Detection is introduced as a separate Process with its associated lower-level components, i.e. Phases and Sub-Phases. This is due to the fact that forensic investigators can never know whether each system they work on has digital investigation readiness activities implemented or not. Figure 24 represents the UML Activity Diagram of the Incident Detection Process.

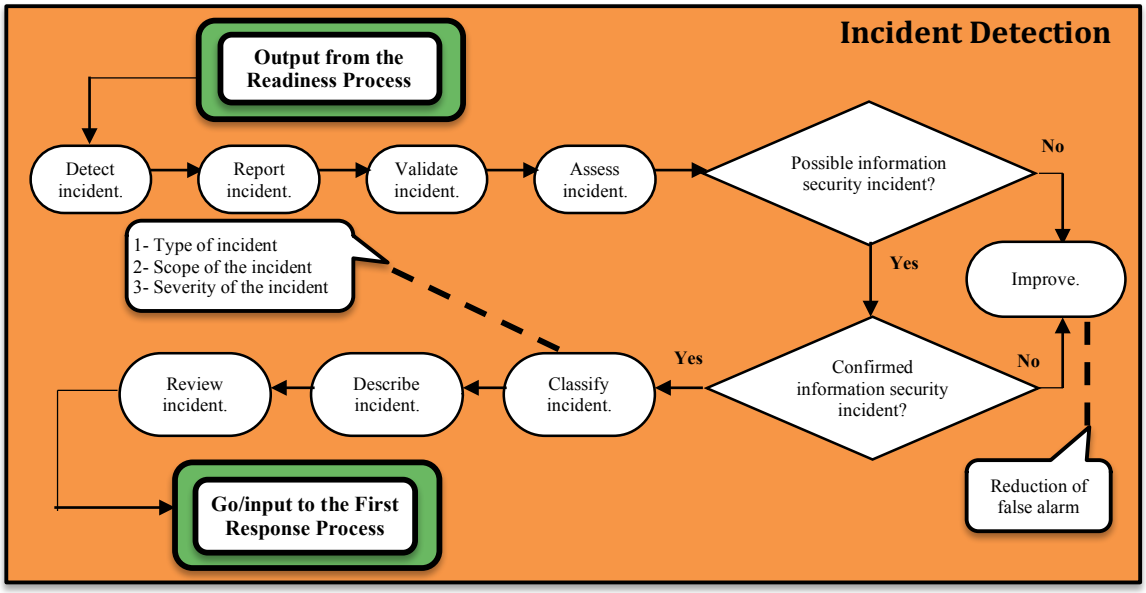


Figure 24. The UML Activity Diagram of the Incident Detection Process

3.6.1.1 Incident Detection Process Components

During the Incident Detection Process, an incident is detected by either internal or external events. Internal events include, but are not limited to, intrusion detection system, intrusion prevention systems, log-analysing systems and change-tracking systems. An example of external events includes crime being reported to the police. After the incident is detected, it should be reported to the relevant individuals or authority such as the management in the company or the law enforcement. The incident will then need to be assessed to confirm or refute its occurrence. If its occurrence is refuted, the improvement will need to be made to ensure the reduction of false alarms. However, if the occurrence of the incident is confirmed, the incident will then need to be classified and described to determine its type.

Authors of the existing models have neither discussed nor assigned any component to the Incident Classification and Incident Description within their models. They simply reduce their discussions to the statement that incidents need to be detected without elaborating on this process. This is a grave weakness because the events causing the investigation could significantly determine the type of investigation required. For instance, the digital investigation could take a completely different course if the incident were categorized as using the computer to distribute child pornography than if it were classified as an unauthorised access to the root account of the operating system. Therefore, since Incident Classification and Incident Description could have significant impact on the rest of the Processes in a digital investigation, two separate Phases, namely Classify Incident and Describe Incident, have been assigned to these two components. Investigators must ensure that these two Phases do not contain any activity that might modify data at the information system where the incident has taken place. This is to ensure that the digital evidence can be preserved. Finally, the incident needs to be reviewed. The output of the Incident Detection Process becomes an input to the First Response Process, discussed in the following section.

3.6.2 First Response Process

In the CDFIPM, the First Response Process only applies to the investigations within corporate settings and not to the law enforcement investigations. This is why some

Phases within the CDFIPM's First Response Process and Secure and Evaluate Crime Scene Process (See Section 3.7.1) might appear to be repetitive at first glance. In corporate settings, often organisations have their own in-house first response team who are called upon to respond to an incident or crime that has targeted an organisation's resources or employees of that organisation. Thus, when an incident is detected within the corporate setting, the first people who respond to the incident or crime are the organisation's own response team. In contrast, in a law enforcement investigation, digital forensic investigators are often called upon to assist individuals or organisations outside of law enforcement who have become the victim of a crime.

The rationale for developing two different processes associated with the first response activities is due to the context in which the investigation is carried out and also the ordering of events. Thus, in the CDFIPM, the First Response Process is the initial step that the first responders within corporate settings must take to respond to the incident that has been detected. Due to the fact that incident response and digital forensics domains overlap (Freiling and Schwittay, 2007), the first response to an incident or crime should fall within the scope of any digital forensic investigation. Therefore, the First Response Process has been incorporated into the CDFIPM to enable the first responders to ensure the integrity of potential digital evidence in corporate investigations.

Unlike the previous DFIPMs, in the CDFIPM, the First Response is a multi-layered process which contains both phases and sub-phases. In almost all of the existing DFIPMs, no lower-level components have been defined under the First Response Process. This might be due to the fact that specifying Phases and Sub-Phases for this Process is a difficult task to achieve as these can vary significantly depending on the type of target information system and the data contained in the target information system. Another reason for this might be due to the fact that many researchers within the domain of digital forensics view incident response and digital forensics as two complete separable fields. Although the scope of the First Response activities could include a whole new project, nevertheless the thesis author has attempted to identify generic Phases and Sub-Phases which could be relevant to all types of target information systems. The identification of lower-level details for the First Response Process of the CDFIPM has been achieved by relying mainly upon the field of Incident

Response as well as feedback acquired from experts operating within this field. Figure 25 represents the UML Activity Diagram of the First Response Process contained within the CDFIPM.

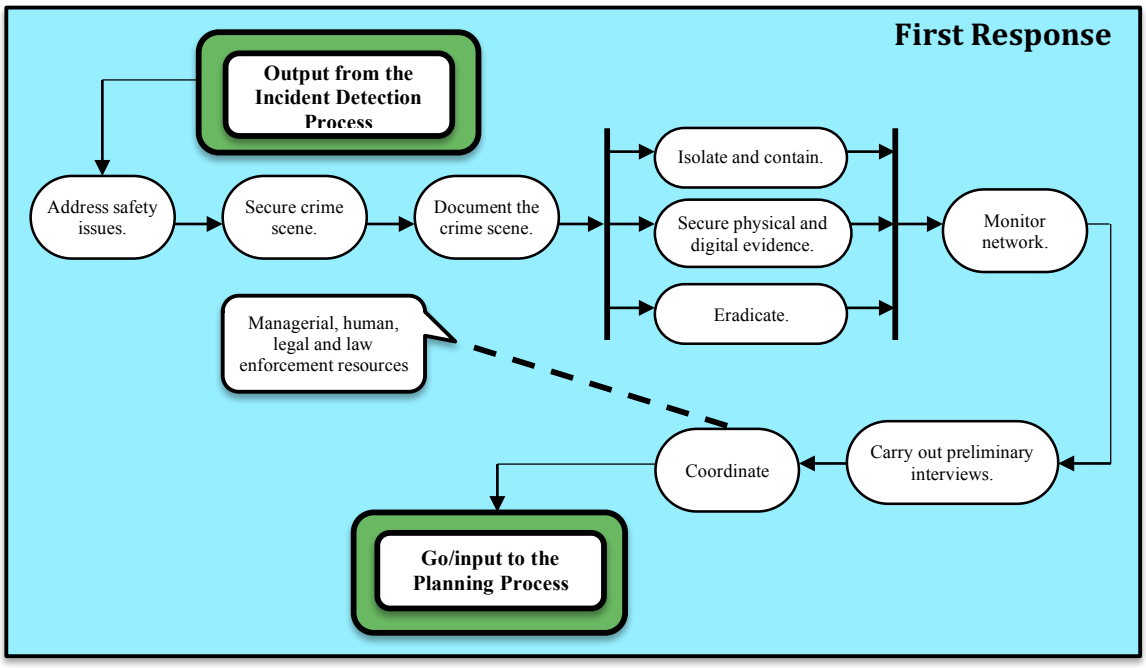


Figure 25. The UML Activity Diagram of the First Response Process

3.6.2.1 First Response Process Components

The starting point to the First Response Process is to address safety issues concerning personnel, witnesses and equipment. The next step is for the first responders to secure the crime scene in order to ensure preservation of the digital device(s) suspected of containing potential digital evidence. Preserving the crime scene will enable better identification and collection of evidence at a later stage. An example of preserving the crime scene can pertain to a server intrusion where the incident response team must determine who was in the data center and prevent others from entering the scene since an employee could be responsible for the incident. At all times during the First Response Process, all activities must be recorded through the Documentation Phase. Based on the type and severity of the incident, the preservation should include disconnecting the digital device from a networked environment if it is connected to a network, detecting the corrupted data, and securing potential physical and digital evidence. Moreover, the network needs to be monitored to detect incoming calls and IP addresses etc. During this process, first responders must describe the scene of the

incident accurately in the initial drafting of documentation using photographs, video and sketches. Contingent on the type of investigation and authorisation, preliminary interviews should be carried out with the suspect to gain knowledge which could assist the investigation. Under the Coordinate Phase, human resources should be coordinated by arranging for the relevant personnel to participate in the investigation. The output of the First Response Process becomes the input to the Planning Process, discussed in the following section.

3.6.3 Planning Process

The Planning Process is one of the most important processes in a digital investigation and is often common across different fields in which DFIs operate. Casey emphasizes the importance of this Process, stating that planning is crucial in particular in circumstances where computers are involved (Casey, 2011). Since the Planning Process can have a significant impact on the efficiency and success of all the other stages in a digital investigative process, a 'discrete' Process has been assigned to the Planning in the CDFIPM. In the existing DFIPMs, Planning and Preparation are often used interchangeably to refer to the same Process incorrectly even though they are two different Processes. In line with ISO/IEC 27043 (2015), Planning and Preparation have been distinguished and assigned two discrete Processes in the CDFIPM, with each Process being refined with lower-level details, i.e. Phases and Sub-Phases.

An exception to the existing DFIPMs where Planning and Preparation are considered the same Process is the model developed by Valjarevic and Venter (2015), in which Planning and Preparation are considered two separate Processes. However, Planning and Preparation Processes in Valjarevic and Venter's model do not provide any lower-level components necessary to assist DFIs in conducting forensically sound digital investigations. Regarding the Planning Process, Sammes and Jenkinson (2007), as cited by Adams (2012), state that it is very important that the number of computers, their types, operating systems and connections are all known before entering the scene of crime. Although this might be true to a large extent in an ideal world, DFIs often have little idea about the computer systems, quantity and location of data, types of hard disk or the operating systems involved, prior to visiting the crime scene (Adams, 2012).

Also, because the initial information concerning the specific online environment might be scarce, insufficient or imprecise, the Planning Process must therefore focus on preparing for as many likely scenarios as possible (Adams, 2012, Brown, 2006). Therefore, it would be unreasonable to expect DFIs to produce anything beyond a rough outline of a plan at this stage of investigation, a view supported by Adams (2012).

In the existing DFIPMs, the Planning Process often requires DFIs to plan only for the activities that need to be carried out at the crime scene. However, the Planning Process in the CDFIPM provides guidance on the potential planning that DFIs should carry out during the entire investigative process. Various considerations need to be made at the Planning stage even though DFIs have little understanding of what they should expect. This includes constructing the relevant procedures, defining methodologies, the choice of tools to be used, planning for the use of appropriate human resources that should be involved in the investigation, and planning all activities during other Processes. In some circumstances, DFIs also need to plan for some 'on-scene' processing of digital evidence (Casey, 2011; Rogers et al., 2006). For example, when DFIs do not have authority to seize every computer system, investigators must perform some on-scene keyword searching of many computers to identify which ones are relevant to the investigation. Another example includes planning for 'onsite triage' where an on-scene examination of a digital system will be required in cases such as child abduction.

Since it is not feasible to develop specific planning tailored to every possible situation (Kent et al., 2006), the Planning Process in the CDFIPM has focused on generic activities so that it can be suitable for different investigations. In circumstances where digital device has already been seized by law enforcement officers and presented to the laboratory for examination, this Process will become brief as it will not be necessary to preform many of the preceding activities (Adams, 2012). Also in the CDFIPM, the Planning Process and Readiness Process are different in that the activities in the Readiness Process are planned and implemented by the organisation, whereas the Planning Process is carried out by the DFIs who draw their own plan of actions. However, if the digital investigation readiness measures were implemented correctly, then the DFIs should plan how to use the results of those measures in order to maximise the success of the digital investigation process.

Figure 26 represents the UML Activity Diagram of the Planning Process followed by the description of its lower-level components.

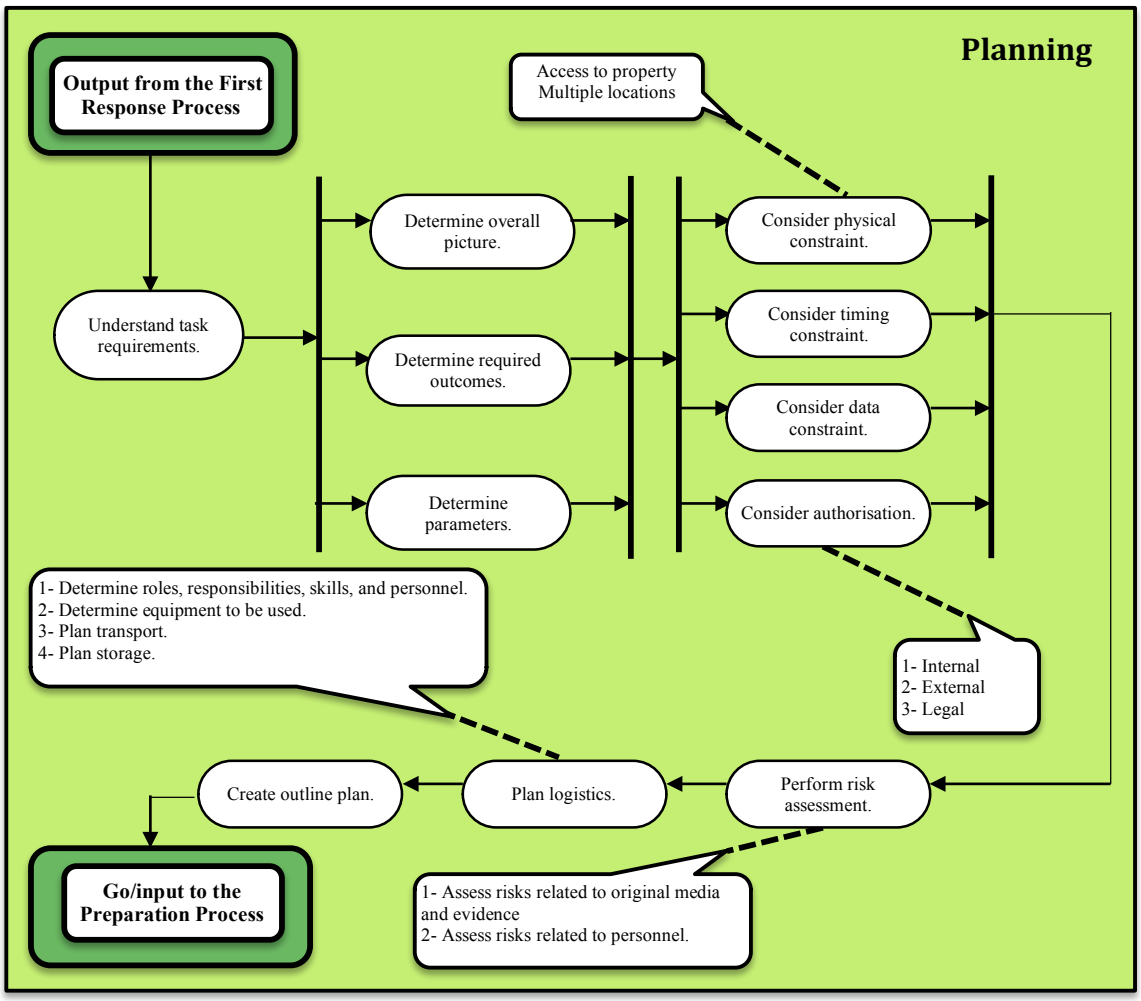


Figure 26. The UML Activity Diagram of the Planning Process

3.6.3.1 Consider Physical Constraint

The Physical Constraint Phase (Adams, 2012) refers to the access to the physical location of the system in which data is held. Previous research, as cited by Adams (2012), has paid little attention to the importance of the Physical Constraint in a digital forensic investigation (Wiles, 2007; Jones et al., 2005; Steel, 2006). Since DFIs might encounter more than one location in which data can be found, "Consider Physical Constraint" has been assigned a discrete Phase in the Planning Process of the CDFIPM. The Physical Constraint Phase consists of two Sub-Phases, namely Access to Property and Multiple Locations, which need to be considered prior to the start of the CDFIPM's Secure and Evaluate Crime Scene Process (discussed in section 3.7.1) (Adams, 2012).

Access to Property

This Sub-Phase involves physical access to the resources where data is being contained. The need to have a physical access to the resources containing data is the case in the majority of circumstances. However, obviously, there are cases in which data can be accessed through the Internet or external networks[24]. Commercial buildings often have security measures in place necessitating keys, cards or door access codes to allow the access to the building. Private sites might have restricted access and parking with security gates. Therefore, lawyers may need to discuss the entry with the occupants so that they can enter and serve the instructions and initiate the CDFIPM's Secure and Evaluate the Crime Scene Process (Adams, 2012).

Multiple Locations

Data might be held at resources at more than one site or at different offices across multiple floors in the same site. Thus, Multiple Locations has been included under Consider Physical Constraint as a Sub-Phase to enable the investigative team to determine how many sets of equipment is required and how many DFIs are needed to attend the scene to carry out the digital data acquisition (Adams, 2012).

3.6.3.2 Consider Timing Constraint

A 'Consider Timing Constraint' has been suggested as a Phase within the Planning Process due to its significance (Adams, 2012). Although some of the previous research and standards discuss practical considerations to some extent (ISO/IEC 27043 2015; Kohn et al., 2013; Casey, 2011 and 2004; Wiles, 2007), they do not include the timing as part of the Planning. The CDFIPM requires DFIs to consider three elements of timing constraint including: 'court orders and warrants', 'private sites' and 'commercial sites' (Adams, 2012). In relation to court orders and warrants, these often impose time restrictions within which the Acquisition Process must be carried out regardless of whether the process has actually been completed or not. Concerning the circumstances where private premises are involved, the investigators might need to arrive at the scene before the subject of investigation leaves the premises but preferably after the partners and/or children have left the building (Adams, 2012).

[24] In cases of accessing data through external networks, there must be a justifiable reason why data needs to be accessed remotely as opposed to employing a DFI onsite to access the data.

Also, in cases where commercial premises are involved, a key holder will need to arrive and provide the investigators with access to the offices after they have checked the court orders or warrants. In cases of covert investigations where the subject of the investigation should be left unaware of the investigation or the need to avoid business disruptions, DFIs are often required to arrive at the premises after working hours and complete the acquisition of the data before employees return (Adams, 2012). This ensures that business flow is not disrupted or the suspect is not able to destroy data representing potential digital evidence. The business disruption element has been considered also by other researchers including Sammes and Jenkinson (2007), as cited by Adams (2012). For instance, Sammes and Jenkinson (2007) recommend a search briefing which consists of both the assignment of tasks and the key objectives as well as recognition of the provisions of the warrant or court order. Adams (2012) state that in cases where data is held at various sites, an appropriate period of time must be permitted so that all the forensic teams will be able to match their arrival to ensure that no individual is informed of the investigation before a team have arrived.

3.6.3.3 Consider Data Constraint

In the context of the 'Consider Data Constraint Phase' (Adams, 2012), data is the digital information which represents the potential digital evidence that is the subject of the Acquisition Process. Data can take various forms such as a text file, a still image and video or audio file, etc. As with other Phases and Sub-Phases of the Planning Process in the CDFIPM, it is not often obvious at the beginning whether there will be any data associated with the investigation or where this data can indeed be found. Various authors in the previous research have provided a list of different types of digital data and recommended different location in terms of where data can be found (Casey, 2011; Marcella and Menendez, 2007; Jones et al., 2005; Farmer and Venema, 2005). Although this level of detail is not included in the proposed model, the CDFIPM nevertheless suggests three data elements regarding possible quantity of data which might be needed, as originally suggested by Adams (2012). These are set out below.

Identification of Data

Prior to data acquisition, it might be required that a DFI previews data through a write-blocking device using certain specialist software which he has already installed on a

forensic workstation. In such cases, the DFI must consider the means of identifying data which will be relevant to the investigation (Adams, 2012). One of the considerations that DFIs should take is to apply appropriate techniques when attempting to identify the relevant data. For example, if the data representing potential digital evidence was in an image format, it would then be inappropriate for DFIs to use a search term to find such a data. The activities performed under this Sub-Phase have an important effect on the times needed to carry out the investigation (Adams, 2012).

Amount of Data

The amount of data that needs to be acquired will have a direct impact on the amount of storage space as well as the amount of time required to perform the data acquisition itself (Adams, 2012). Although nowadays even a large disk space is rather inexpensive, there might be difficulties concerning physically managing a large number of disks. In cases of the live acquisition of data, it is very probable that the network performance will be affected negatively (Adams, 2012). Therefore, DFIs will need to ensure that they communicate the impact of this to the clients and lawyers in order for the effect on the business holding the data to be considered. This might result in negotiations in terms of how and when the live data acquisition will be performed (Adams, 2012).

Location of Data

Data location varies; there are certain data locations which might be challenging to DFIs such as data held on backup tapes or held by a third-party provider of a cloud solution. In cases of the backup tapes, DFIs will need to take into account the appropriate means of restoring the relevant backup tapes or consider putting into place a plan to remove and duplicate the tapes offline (Adams, 2012). Providing the details of such operation is outside the scope of the CDFIPM. Concerning the data that is held by a third-party as part of cloud solution, the data obviously should be accessed via the Internet. This poses various challenges especially regarding authorisation; also in terms of geographical location, it is also possible that DFIs might not be able physically to access the place in which data is stored (Adams, 2012).

3.6.3.4 Consider Authorisation

DFIs need to ensure that they have the proper authorisation to be able to conduct the work. The type of authorisation required for an investigation to proceed will not be known unless the type of investigation is determined first. The authority can include both internal and external authorizations (Ciardhuáin, 2004). Internal authorisation can come from the organisation which provide the services whereas the external authorization is the authority in law and the authority from the owner of the resources which contain the material to be acquired (Adams, 2012).

Internal Authorisation

Depending on the specific organisation involved, the internal authorization has different forms. If the provider of the digital forensic services is a small organisation, the procedure of the internal organisation is rather straightforward and could include a signed agreement specifying the services intended to be provided. In contrast, for a large organisation which might be part of a larger service provider, the process of authorization is often more complicated. In this case, different conflicting instructions and risk assessments will be required to be carried out in order to reduce conflicts of interest which focus on legislative regulations or commercial considerations (Adams, 2012). Previous research, as cited by Adams (2012), assumes by default that DFIs are employed in the organisation which owns the resources to be investigated and therefore presume that the authorization has already been granted (Wiles, 2007; Steel, 2006). However, this previous research has not covered the third-party providers of digital forensic service in relation to process models (Adams, 2012).

Authority in Law

DFIs who operate within the field of commerce are required to ensure that they have acquired proper legal authority to offer the services in a way that they have been requested. This might involve the investigators' names being placed on the court orders or other documents (Adams, 2012). In terms of DFIs who work within the field of law enforcement, they will need to confirm the details of the proper authorization and any restrictions imposed. Moreover, DFIs will need to examine any court orders closely allowing access to a third party's property. This is because if DFIs conduct any action that is not allowed by the law, they may become the subject of lawsuit themselves.

DFIs must also take into account the potential discovery of materials which are covered by the criminal law such as child pornography. If such materials are found, DFIs will need to inform the client of such a discovery and consult the appropriate law enforcement.

External Authority

If a DFI has been asked to conduct the investigation for a company, the system of which needs to be accessed, the DFI must ensure that the individual(s) who provides instructions is allowed to access the system involved. This is because data from more than one entity might have been stored on a single computer system. For example, the resources might be held at a third-party provider of IT services (Adams, 2012).

3.6.3.5 Create the Outline Plan

The outcome of all the Phases and their associated Sub-Phases within the Planning Process will be the Create the Outline Plan Phase. Since DFIs have not yet attended and surveyed the crime scene at this stage, only a rational prediction can be made with certain contingency plans being put in place. For example, some personnel need to be tasked with remaining on standby to collect and deliver additional storage devices, application software or other resources (Adams, 2012). Some researchers have previously considered the creation of the outline plan. For example, Sammes and Jenkinson (2007) implicitly refer to the creation of the outline plan by discussing a "Search Briefing". Although Sammes and Jenkinson (2007), as cited by Adams (2012), approach the search briefing from the point of view of law enforcement, this activity is still relevant to the commercial field as well. This is because it ensures that all individuals implicated know about the available information at the time including any constraints imposed by court orders or other authorities (Adams, 2012).

According to Sammes and Jenkinson (2007), DFIs should be able to address the following questions:

1. How many trained personnel are needed?
2. How many teams are required; where do they need to be and at what date/time?
3. How many sets of equipment are required, and what should be in the toolkits?

4. What specialist skills are required (e.g. someone with mainframe server knowledge may need to be at a specific location)?
5. How much storage media is required at each location, and how can this be supplemented if necessary?
6. Will the services of another employee/contractor be required (e.g. a system IT administrator to assist with shutting down servers or locating backup tapes)?

Adams (2012) is more explicit about the need for the creation of an outline plan and suggests six main types of activities as follows:

- The number of trained investigators needed;
- The type and set of equipment needed at each site including software, dongles, write-blockers and image storage media;
- The start time at each site and the estimate of the duration of acquisition stage;
- The details of personnel involved including contact numbers of team leaders/lawyers/client liaison distributed;
- The acquisition plan detailing target storage locations, protocol and key words; and
- The applicable constraints – authorisation, physical, timing and data.

Therefore, the Create Outline Plan of the Planning Process must detail the activities suggested by Adams (2012) and Sammes and Jenkinson (2007) as described above. Providing the details about what needs to be included in the toolkit that should be taken to the crime scene is beyond the scope of the CDFIPM. Valuable resources providing detailed description of what equipment needs to be taken onsite can be found in the research conducted by Sammes and Jenkinson (2007), Brown (2006) and Jones et al. (2005). It is argued that the content of the toolkit which needs to be taken to the crime scene should be determined by DFIs themselves (Adams, 2012).

3.6.4 Preparation Process

Preparation Process involves implementing the planning and procedures outlined in the Planning Process. The aim of this Process is to prepare the organisation and DFIs for

carrying out the activities in the following Processes in the CDFIPM. This includes, but is not limited to, preparing appropriate equipment (both hardware and software), infrastructure, human resources, raising awareness, training and documentation. Figure 27 represents the UML Activity Diagram of the Preparation Process.

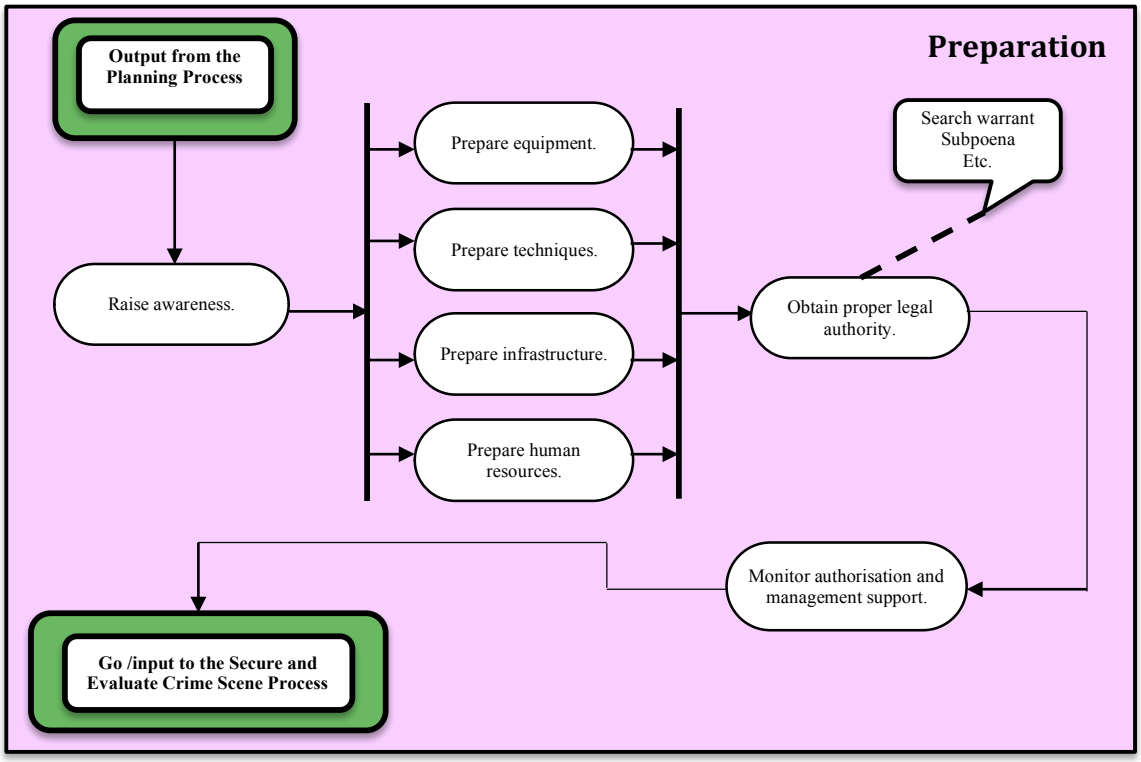


Figure 27. The UML Activity Diagram of the Preparation Process

Although Preparation has been assigned a discrete Process, it has also been considered as an Overriding Principle within the CDFIPM. The discrete Preparation Process refers to the generic preparation necessary throughout the investigation. In contrast, Preparation as an Overriding Principle refers to the preparation that DFIs should carry out for each given Process concurrently throughout other Processes within the CDFIPM, a view supported by Casey (2011), who states "Preparation is needed at every step of an investigation." Preparation Process has been included in the CDFIPM to enable DFIs to be better equipped to conduct more effective digital investigations. Moreover, it will ensure that the integrity of potential digital evidence is not compromised because of the lack of possible preparedness by DFIs.

3.7 Acquisitive Processes Class

Acquisitive Processes Class represents the first layer of the CDFIPM, the aim of which is to secure the crime scene, identify, acquire and collect both physical and digital evidence. Similar to other Classes of the CDFIPM, the Acquisitive Processes Class is also multi-layered containing three further lower layers including Processes, Phases and Sub-Phase. There are three Processes included in the Acquisitive Processes Class consisting of Secure and Evaluate the Crime Scene, Identification, and Acquisition and Collection. This section describes these Processes and their associated lower layers, namely Phases and Sub-Phases. Figure 28 represents the UML Activity Diagram of the Acquisitive Class Processes in their abstract level.

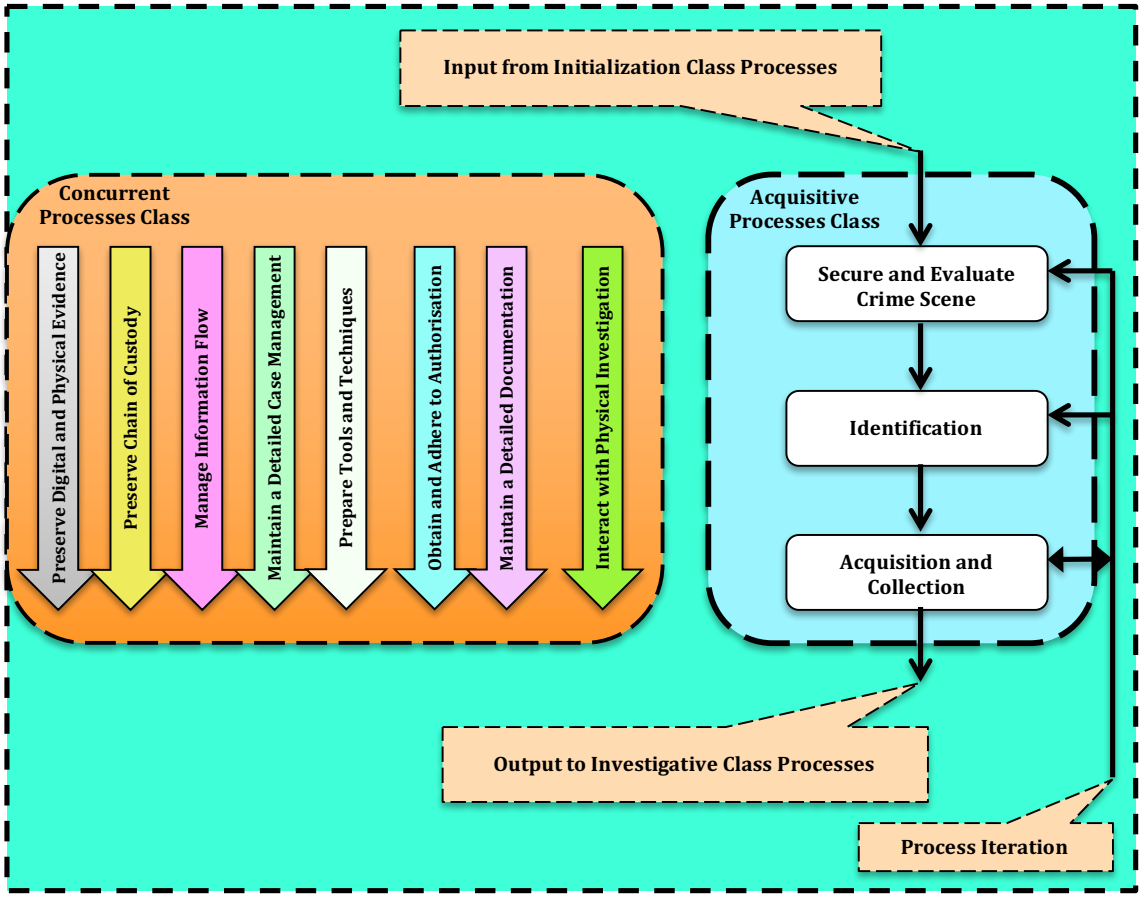


Figure 28. The UML Activity Diagram of Acquisitive Class Processes in their abstract level

In the following sections the Acquisitive Processes Class will be broken down to describe its lower-level components, namely Processes. In turn, each Process will be further refined in greater detail to specify and describe its lower-layer components, i.e. Phases and Sub-Phases.

3.7.1 Secure and Evaluate Crime Scene Process

Once the proper planning and preparation have been finalised, DFIs will now need to attend the crime scene where the data representing potential digital evidence might be stored in a digital system. At this stage, the Initialisation Process moves to those Phases that directly deal with the actual suspect and the crime scene. During this stage, an outline plan for the subsequent Acquisition Process is created. In order to demonstrate in a court that the digital evidence was acquired in a forensically sound manner, first DFIs must be able to show that the crime scene from which the digital evidence was acquired was left unaltered. Thus, there must be a distinct process which details the steps that DFIs should undertake prior to the 'identification' and 'acquisition' of digital evidence in order to preserve the crime scene securely. Lack of such a discrete Process is most likely to invite challenge to the way that the digital evidence has been acquired and ultimately render the incriminating evidence futile.

Unfortunately, the authors of the existing models have inappropriately skipped this vital stage of digital investigation by not assigning a separate Process to 'Securing the Crime Scene' prior to the 'Identification' and 'Acquisition' Processes. They have often reduced their discussions to the statement that digital evidence needs to be identified and acquired without providing necessary details on the steps required to be undertaken by DFIs prior to the identification and acquisition of digital evidence. In the existing models, often one single Process is assigned to cover the three elements of 'Preservation', 'Identification' and 'Acquisition'. Although some authors such as Casey (2011) have discussed preserving the crime scene briefly, they have not provided an explicit Process to accommodate the activities related to securing the crime scene.

Therefore, the Secure and Evaluate Crime Scene Process with its associated lower-level components has been designed and incorporated into the CDFIPM as a separate Process to assist DFIs in securely preserving the crime scene prior to the Identification and Acquisition Processes. The development of this Process is another novel contribution of this research to the field of digital forensics. Other two separate Processes of the CDFIPM, namely Identification and Acquisition (discussed later), with their lower-level details that will need to be carried out at the crime scene are further contributions of this research to the field of digital forensics. Figure 29 represents the UML Activity

Diagram of the Secure and Evaluate the Crime Scene Process followed by the description of its Phases and Sub-Phases.

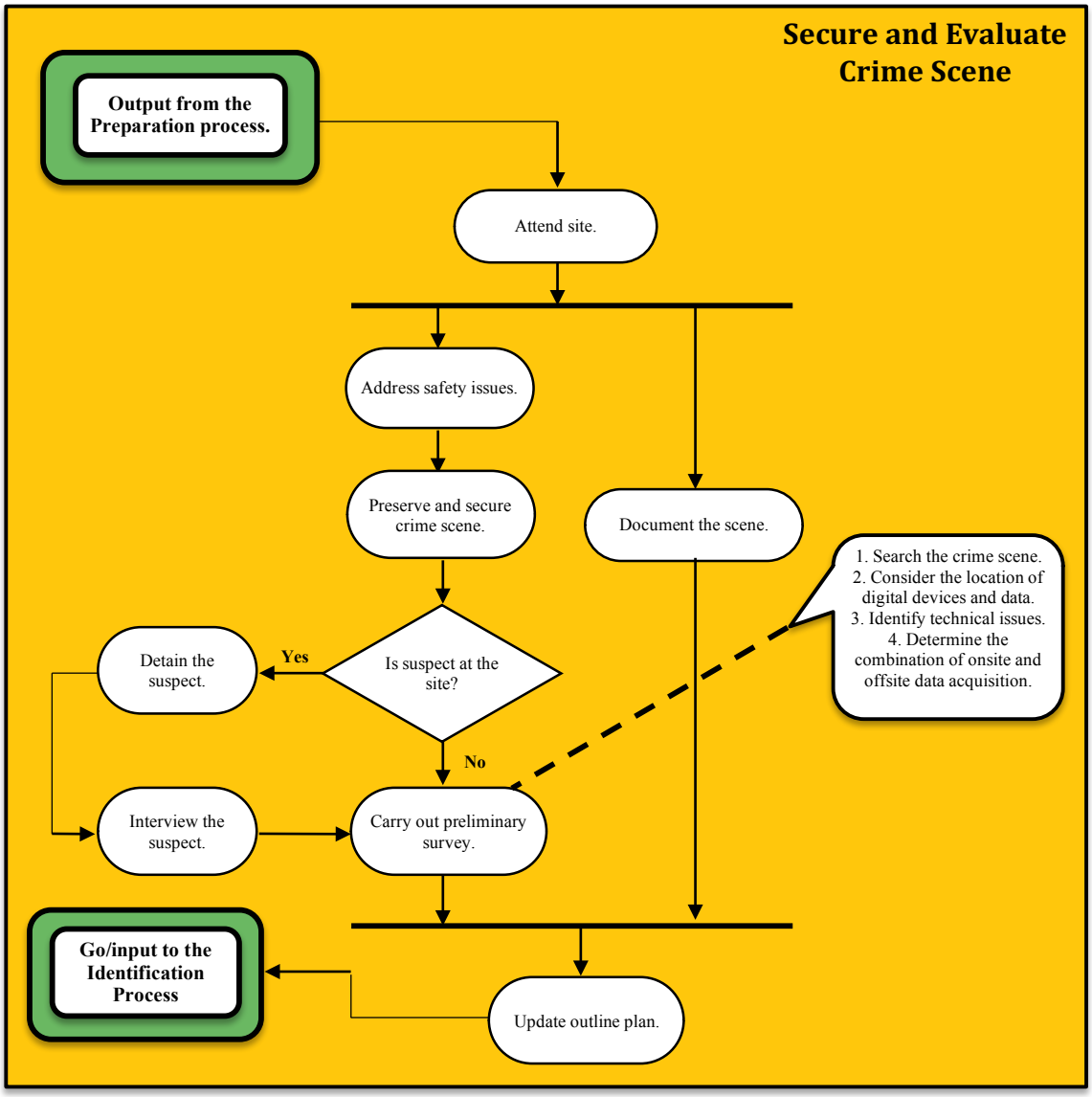


Figure 29. The UML Activity Diagram of the Secure and Evaluate Crime Scene Process

3.7.1.1 Address Safety Issues

In line with ACPO (2012) Good Practice Guide, Adams (2012) and Brown (2006), the CDFIPM requires the investigators to address the safety issues prior to conducting any of the Phases of the Secure and Evaluate Crime Scene Process. Safety issues should cover both investigators and witnesses as well as the materials under the investigation.

3.7.1.2 Preserve and Secure Crime Scene

In order to demonstrate in a court that the activities associated with the Secure and Evaluate the Crime Scene Process were carried out in a forensically sound manner, DFIs must be able to show that the crime scene was preserved unaltered. Thus, if possible and practicable, the investigators must enforce a lock down of the entire crime scene in order to achieve what Casey (2011) calls a "pristine environment" to preserve the integrity of both the digital device(s) and the potential evidence contained in it. Other steps that DFIs should take include preventing individuals from entering or leaving the crime scene, and preventing unauthorised people (including the suspect) from tampering with the digital device and materials under investigation.

In terms of preserving the digital crime scene, this can include, but is not limited to, blocking the network connectivity. A computer system attached to a network that is running can be regarded as fragile evidence due to the fact that its data representing potential digital evidence could be deleted with commands from a remote system. Examples of procedures to preserve the content of a computer in this situation are to unplug the computer from the network when it is found, or to utilise a network monitor to view what data is being sent to the system until the full investigation begins (see also section 3.6.2 for an example of preserving the crime scene in corporate investigations).

3.7.1.3 Interview the Suspect

Interviewing the suspect is an extremely important aspect of the Secure and Evaluate the Crime Scene Process. If the investigation is not covert and the suspect is at the crime scene, he/she must be detained and interviewed. Suspects often would be psychologically more vulnerable within the first few hours of their initial encounter with the police (Black, 2014), particularly when this encounter takes place in their place of business or dwellings (Yeschke, 2002). Due to the shock that they have received, they often tend to be more compliant and open to answering the police questions even after they have been "mirandized" (Rogers et al., 2006; Memon et al., 2003). Based on an examination of 600 taped police interviews of suspects in England, Baldwin (1993) reported that in the majority of cases (80 per cent), suspects were thoroughly

cooperative and answered police questions of any significance in the initial periods after the raid into their dwellings or places of work.

Therefore, investigators should capitalize upon the initial status of the suspects and their willingness to cooperate in order to extract information that could assist the ongoing investigation. Such a compliance could be crucial in certain circumstances such as abductions and sexual predatory offenses. At this stage into the investigation, what is critical to the investigators is the knowledge of the full extent of the crime or involvement of the suspect and triggers that further increase the suspect's willingness to talk and cooperate. These triggers might originate in the digital evidence stored on the suspect's digital device such as email correspondence, digital maps, pictures and chat logs. It is very important that investigators and interviewers who are dealing directly with the suspect provide direct input to the digital forensic examiners at this stage. This ensures that correct prioritizations and assumptions are being made in relation to the potential digital evidence identification and acquisition activities.

3.7.1.4 Carry out the Preliminary Survey

Once the crime scene has been securely preserved, investigators attending the crime scene will need to conduct a 'preliminary survey' of the physical crime scene to obtain an idea about how to process the physical and digital crime scenes and what kind of special skills are required. The aim of the Carry out the Preliminary Survey Phase is to collect and analyse the physical evidence and reconstruct the events that occurred during the incident or crime. The fundamental purpose of a digital investigation is to identify people responsible for an incident or crime; therefore, physical evidence is needed. In the context of law enforcement investigations, a physical crime scene expert often works alongside the primary investigators and digital forensic investigators. In corporate investigations, the response team or the physical security team might need to complete the activities under this process.

In terms of surveying the physical crime scene, investigators should walk around the crime scene to identify obvious pieces of evidence and pieces of evidence that might be short-lived. During this Phase, initial observation of who, what, where, when, and how needs to be documented, and an initial theory must be developed. Although conducting

a preliminary survey is vital while attending the crime scene, the existing research has hardly paid attention, if any, to a systematic search for and identification of the digital devices containing potential digital evidence. Those authors who have spent efforts discussing the survey of the crime scene have simply sufficed their discussions to the fact that the digital device containing potential digital evidence must be identified without elaborating on the details. Therefore, to address this issue, in the CDFIPM, a discrete Phase, Carry out the Preliminary Survey, has been designed and incorporated into the Secure and Evaluate Crime Scene Process aiming to enable the DFIs:

- to identify the obvious pieces of physical evidence by walking around the crime scene (Casey, 2011; Carrier and Spafford, 2003);
- to identify the fragile pieces of physical evidence that might be short-lived (Carrier and Spafford, 2003);
- to identify any technical issues (Adams, 2012);
- to survey the digital crime scene to identify data of interest that represents potential digital evidence;
- to determine the mixture of onsite and offsite acquisition (Adams, 2012); and
- to develop and initial theory about the incident or crime.

Newman (2007) and Carrier and Spafford (2003) have suggested various activities that DFIs will need to undertake while surveying the physical crime scene. These activities have been refined and incorporated as 'Sub-Phases' into the Secure and Evaluate the Crime Scene. The activities in question that DFIs should undertake when surveying the physical crime scene include:

- determining all the locations that might need to be searched;
- identifying the number and location of computers, what network connections the computers have, PDAs, cell phones, passwords on pieces of paper, and CD-ROMs or other removable media;
- identifying any specifics that must be addressed relating to hardware and software;
- identifying possible personnel and equipment needs for the investigation;
- determining which devices can be physically removed from the site; and

- identifying all of the individuals who had access to the computer or digital resources.

The outcome of this Phase should be that the investigators have acquired an idea about how they should process the physical crime scene and what special skills are required. A computer system that is running and plugged into a network can be considered as fragile evidence (Carrier and Spafford, 2003) since its digital evidence could be deleted with commands from a remote system. Thus, some measures include unplugging a computer from the network when it is found or deploying a network monitor to view what data is being sent to the system until the full investigation begins (Carrier and Spafford, 2003).

3.7.1.5 Update the Outline Plan

After carrying out all the Phases of the Secure and Evaluate the Crime Scene Process, investigators will need to review and update the outline plan now that its various assumptions can be assessed (Adams, 2012). Often, there will exist areas of the plan that could not be completed at all during the Planning Process before attending the crime scene where potential digital evidence can be found.

3.7.1.6 Document the Scene

It is extremely important to document all of the activities carried out throughout the Secure and Evaluate the Crime Scene Process in order to enable other investigators to authenticate the process and results. It is therefore imperative to maintain a detailed record of what was performed on the computer system and what information was acquired. Maintaining a detailed documentation will enable DFIs:

- to preserve chain of custody in a forensically sound manner;
- to increase the possibility of a successful investigation; and
- to record all information produced during this process to support decision making and the legal, administrative processing of those decisions.

During the Document Phase, DFIs will need to take photographs, sketches and videos of the crime scene (both physical and digital). The aim of this Phase is to obtain as much information as possible in order to preserve and record the layout and vital details of the crime scene. For instance, investigators will need to document and photograph the connections on the computer and the state of the computer. Also, if possible, investigators should also document the number and size of the hard drives and the amount of memory. In some cases, as suggested by Carrier and Spafford (2003), investigators must record the hardware MAC address of the network cards in order that DHCP logs can be used to identify system activity. It might also be useful to record serial numbers and asset tags during this phase. As a general principle, investigators must record anything that could be valuable to the DFL and subsequent reconstruction. Some authors (Carrier and Spafford, 2003) have suggested that Chain of Custody forms must also be created during the documentation. However, this seems to be inappropriate considering the limited time that DFIs have. Moreover, investigating organisations within which DFIs operate should have already developed Chain of Custody forms as part of their Standard Operating Procedures (SOPs).

The Document Scene Phase in the Secure and Evaluate Crime Scene Process is limited only to a single stage in time. In contrast, Documentation as an Overriding Principle (discussed later) must be maintained concurrently throughout the entire investigative process. Finally, the components designed and incorporated into the Secure and Evaluate Crime Scene Process have been defined in such a generic manner so that they can be relevant to both law enforcement and corporate investigations. Because of its level of details and generic approach, the Secure and Evaluate Crime Scene Process provides a smooth transition to the Identification Process of the CDFIPM, discussed in the next section. Also, this Process might become irrelevant in circumstances where a digital device has already been seized and transported back to a DFL (Adams, 2012). In these situations, investigators can simply skip this process without negatively affecting the results of the investigation.

3.7.2 Identification Process

Once the crime scene has been securely preserved, DFIs will need to identify the items that might contain potential evidence related to the investigation. During this stage, all

the gaps in knowledge with regards to the location, size and format of digital systems containing the digital data are filled in (Adams, 2012). McKemmish (1999) highlights the significance of the Identification "Activity" by stating that it is impossible to establish the most appropriate process for the acquisition of digital evidence until the location and storage format of digital evidence are identified Adams (2012). It is, therefore, important to identify potential digital evidence at the crime scene since the identification of digital evidence has a significant impact on the rest of the processes. If DFIs do not identify potential digital evidence at this stage, it might not exist at later stages in the process. This is particularly essential when the crime takes place in a networked environment in which live investigations should be carried out, in a cloud environment or in any environment that involves large amount of data to deal with.

Once the 'potential digital evidence' has been identified, it becomes 'digital evidence' from this point onwards since it has been identified as such during the Identification Process (Valjarevic and Venter, 2015; ISO/IEC 27043, 2015). As with the Secure and Evaluate Crime Scene Process (discussed in the preceding section), in certain circumstances the Identification Process at the crime scene will also become irrelevant when the digital device has already been seized and submitted to a DFL for analysis. In the existing models, the term "identification" has often been used to refer to different types of activities. For example, Kent et al. (2006) refers to "identification" as the recognition of digital devices in a physical crime scene whereas Kohn et al. (2013) use the same term to refer to the identification of the potential digital evidence contained in a digital device. In the CDFIPM, the Identification Process refers to the recognition of both the digital device containing the potential digital evidence and the recognition of the digital evidence itself.

Furthermore, as stated in the preceding section, many of the previous models have not assigned a discrete stage to the Identification Process. Although there are few models which have considered identification as an "activity", they have not provided sufficient details for this process by simply reducing their discussions to the statement that the digital device containing evidence must be identified. Therefore, in the CDFIPM, a more thorough and detailed approach has been taken by creating a discrete Process for the identification of both the digital device and digital evidence that contains lower-level details i.e. Phases and Sub-Phases. In the new model, Identification Process

requires DFIs to search for, identify, prioritize and document digital evidence. Digital evidence can be both in physical and logical form. The physical form refers to the representation of data in a tangible device. However, the logical form includes the virtual representation of data in a device. Figure 30 represents the UML Activity Diagram of the Identification Process, contained in the CDFIPM, followed by the description of its lower-level components i.e. Phases and Sub-Phases.

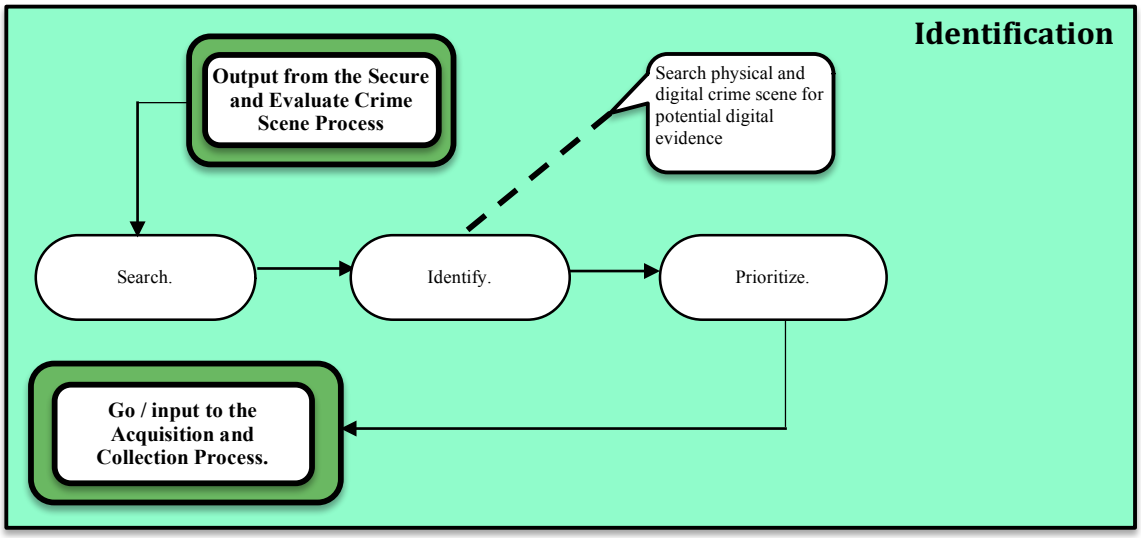


Figure 30. The UML Activity Diagram of the Identification Process

3.7.2.1 Search

This phase involves investigators embarking upon a detailed and thorough search of the crime scene for additional physical evidence to be collected, and also any particulars that need to be dealt with concerning hardware and software now that the initial Carry out Preliminary Survey Phase has been carried out. During this Phase, investigators must use search patterns in order to identify additional evidence that was not discovered in the Carry out Preliminary Survey Phase in the 'Secure and Evaluate the Crime Scene Process'. Investigators will need to use the theory that they developed during the 'Carry out Preliminary Survey Phase' in order to look for particular pieces of evidence that are still missing. Also, because not all of the physical objects can be seized from the crime scene and transported back to a DFL, the Search Phase must be systematic and detailed enough to collect only the required evidence to avoid overloading the DFL with irrelevant objects.

At this stage, the search can be directed towards missing pieces of physical evidence or additional media and digital devices at the crime scene. It is very important that investigators follow a systematic and stringent search patterns during this Phase. The search should also include contacting people to preserve and acquire access logs for doors of a data center, change logs for server updates, firewall logs, IDS logs, and remote access logs. Thus, the Search Phase enables the investigators to conduct a thorough search and to complete essential documentation, and uses the investigators' experience to identify pieces of evidence valuable to the investigation.

3.7.2.2 Identify

The Identify Phase requires DFIs to identify both the storage media and processing devices that could contain potential digital evidence and also the digital evidence itself. Since certain types of digital storage media are difficult to identify and locate, DFIs must ensure that during this process they do not overlook any of the digital devices due to their small size, disguise or blend within irrelevant items. Consequently, it is essential that DFIs methodically conduct a detailed search to identify the devices that could hold potential digital evidence.

3.7.2.3 Prioritize

Due to the fact that in certain circumstances the time is crucial, it is extremely important that DFIs perform some sort of initial prioritisation in which items of evidence or potential containers of evidence that are the most important or the most volatile are dealt with first. The Prioritize phase is central to the Identification Process or indeed the remaining investigation. It is the foundation upon which all the other Processes are built. During this Phase, digital sources that might contain potential digital evidence will need to be prioritised based upon the criteria of potential applicable evidence that can be acquired within a short period of time, and evidence with a short time to live (e.g. data in volatile memory, process tables, routing tables, temporary files systems). One of the benefits of the prioritisation is that it will enable DFIs to ensure the precise order of Phases and Sub-Phases in the Acquisition Process in the next stage so that the digital evidence is not contaminated and DFIs can obtain the best evidence.

3.7.3 Acquisition and Collection Process

3.7.3.1 Considerations towards Data Acquisition Process

The Acquisition Process has a significant bearing on the entire digital investigative process. The Acquisition Process is often challenged by the courts concerning infringements during the chain of custody (Kruse and Heiser, 2001), documentation (Jones et al., 2005), the integrity of the evidence (Brown, 2006) and the methods and procedures utilised to acquire the digital evidence (Kessler, 2010). If the court doubts the initial collection and management of digital evidence, the entire digital investigative process will be subject to dispute. Therefore, since digital evidence might be rendered unusable when appropriate procedures are not adhered to, the CDFIPM requires DFIs to maintain the strict legal regulations during the Acquisition Process. Moreover, since the documentation is of extreme importance, DFIs must ensure that they maintain a detailed record of all the activities that they perform during this process at all times. Prior to describing the Acquisition Process of the CDFIPM, it is important to outline various important points in this section to enable DFIs to conduct data acquisition in a forensically sound manner.

There exist three scenarios in which data acquisition might need to be conducted. These include:

- when digital devices are powered on;
- when digital devices are powered off; and
- when digital devices are powered on but cannot be powered off (such as mission-critical digital devices).

All the three above scenarios have been applied to the Acquisition and Collection Process of the CDFIPM (see Figure 31). In all the three scenarios, DFIs following the CDFIPM are required to make an accurate digital copy of the storage media containing potential digital evidence.

Powered-on Devices

When performing digital evidence acquisition on powered-on digital devices, DFIs must consider the below five baseline activities:

1. DFIs should consider acquiring potential digital evidence that may otherwise be lost if the digital device is powered off. This is also known as volatile data such as data stored on RAM, running processes, network connections and date/time settings.

2. Performing live acquisition is necessary to acquire live data from devices that are still running. Live acquisition of volatile data in RAM may enable recovery of valuable information such as network status, decrypted application and passwords. Live acquisition can be conducted on the console or remotely via the network. The processes are different, and require the use of different sets of tools.

3. DFIs should never trust the programs on the systems. For this reason, trusted tools obtained by DFIs (static binaries) are recommended whenever possible. DFIs should be competent to use validated tools and be competent to account for the effects such tools may have on the system (e.g. displacement of potential digital evidence, or the content of memory being paged out when software is loaded). All the actions performed and the resulting changes made to the potential digital evidence should be documented and understood. If it is not possible to determine the likely effect of introducing tools to the system, or the resulting changes cannot be determined with certainty, this should also be documented.

4. When acquiring volatile data, DFIs should adopt the use of a logical file container, and where possible document its hash value once it contains the volatile data file(s). Where this is not possible, a container such as a ZIP file should be used, and then this file should be hashed and the value documented. The resulting file containers should be stored on a digital storage medium that has been prepared for this purpose, i.e. formatted.

5. In circumstances where it is necessary to acquire non-volatile data from devices that are still running, DFIs must execute the imaging process on the live non-volatile storage using a validated imaging tool. The resulting digital evidence copy should be stored on a digital storage medium that has been prepared for this purpose. The use of digital evidence copies from validated processes ensures the integrity of data when reconstructed. Therefore, whilst it is preferable to use a new digital storage medium, a digital storage medium that has been sanitized will also suffice. If the image has to be stored in a logical file container, DFIs must ensure that the image cannot be corrupted or damaged.

In situations where the device is locked down, physical access may be conducted via other means that has direct memory access enabled, e.g. Firewire interface.

Powered-off Devices

DFIs must consider the following baseline activities when conducting digital evidence acquisition on powered-off digital devices:

1. DFIs must ensure that the device is indeed powered off.
2. DFIs must remove the storage from the powered off digital device if it is not yet removed, label the storage as suspect storage and document all the details such as make, model name, serial number and size of the storage.
3. DFIs must execute the imaging process by using a validated imaging tool to create a digital evidence copy of the suspect disk.

In some cases, the storage media should not be removed from the digital device until data acquisition is performed on the storage media. This is because removing storage media might increase the risk of damage or confusing it with another storage media. Organisations within which DFIs operate should already have their own internal SOPs to follow regarding the need to remove hard disks.

Mission-Critical Devices

In some cases, digital devices cannot be powered off due to the critical nature of the systems. These systems such as servers at data centres that could be serving innocent clients, surveillance systems, medical systems and many others might be critically

affected if they are interrupted or powered off. Special care should be taken when dealing with such systems. In circumstances in which the digital device cannot be powered off, DFIs must conduct live (as discussed previously) and/or partial acquisition. Partial acquisition may be performed due to several reasons such as:

1. The system storage is too large to be acquired (e.g. database server).
2. A system is too critical to be powered down.
3. Only selected data to be acquired contains other irrelevant data within the same system.
4. Data acquisition is constrained by legal authority such as a search warrant that limits the scope of the acquisition.

When a decision has been made to do partial acquisition, the activities for acquisition should include, but are not limited to, identifying folders, files or any relevant proprietary system options available to acquire the desired data, and conducting logical acquisition on the identified data.

3.7.3.2 Contribution of the CDFIPM's Acquisition Process

Before the CDFIPM's Acquisition Process is presented and discussed in the next section, it is also worthwhile discussing in this section some limitations of the existing models in relation to this important process, and also to outline further contributions of this research through the approach taken to address these limitations. One of the shortcomings of the previous models concerning their data acquisition activity is due to the superficial level of details provided concerning this process. These models (e.g. Valjarevic and Venter, 2015; Adams et al., 2014; Kohn et al., 2013; Bulbul et al., 2013, etc.) often provide a high-level, single phase stating that the data needs to be collected without providing lower-level and useful details necessary to assist DFIs in acquiring digital evidence in a forensically sound manner. The activities and techniques of the data acquisition are often left to be determined by DFIs themselves. This has resulted in inconsistencies in terms of the number and types of activities required under this process.

Another limitation of the existing models related to the data acquisition process is the fact that they do not explicitly distinguish 'live' data acquisition from 'static (dead)'

data acquisition where each activity requires a different set of components and procedures. Also, although there are some models that refer to 'live acquisition' to some extent, they often tend to discuss the live acquisition of 'volatile data' without making any reference to the live acquisition of 'non-volatile data' which can be as important. Moreover, the authors of the existing models imply that the acquisition of digital evidence should be performed in an ideal environment such as a DFL. However, in many circumstances such an ideal environment is far from practice, for example in cases of live acquisition where the seizure of the system cannot be authorised. In order to address the stated shortcomings associated with the Acquisition Process, the following considerations were made when designing the Acquisition and Collection Process of the CDFIPM:

- Static acquisition and live acquisition have been differentiated in the CDFIPM; therefore, relevant and discrete components have been assigned to each process.
- The CDFIPM has further distinguished between a static data acquisition onsite and a dead data acquisition in a DFL, and has assigned discrete components to each aspect accordingly.
- The live data acquisition process has been further broken down into both 'live acquisition of volatile data' and 'live acquisition of non-volatile data', and as such relevant components have been assigned to each aspect accordingly.

Thus, in the Acquisition and Collection Process of the CDFIPM, live acquisition pertains to the acquisition of both volatile and non-volatile data from a running device, whereas the dead acquisition relates to the static acquisition of data from a powered-off device onsite or in a DFL. It is contended that the Acquisition and Collection Process developed and incorporated into the CDFIPM is the 'most accurate' and 'detailed' acquisition process presented to date. It is also argued that the CDFIPM's Acquisition and Collection Process has been developed in such a generic way that it could be applied in the different fields of digital forensics and employed for a large number of potential scenarios.

3.7.3.3 Data Acquisition Representation and Discussion

Figure 31 represents the UML Activity Diagram of the CDFIPM's Acquisition Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

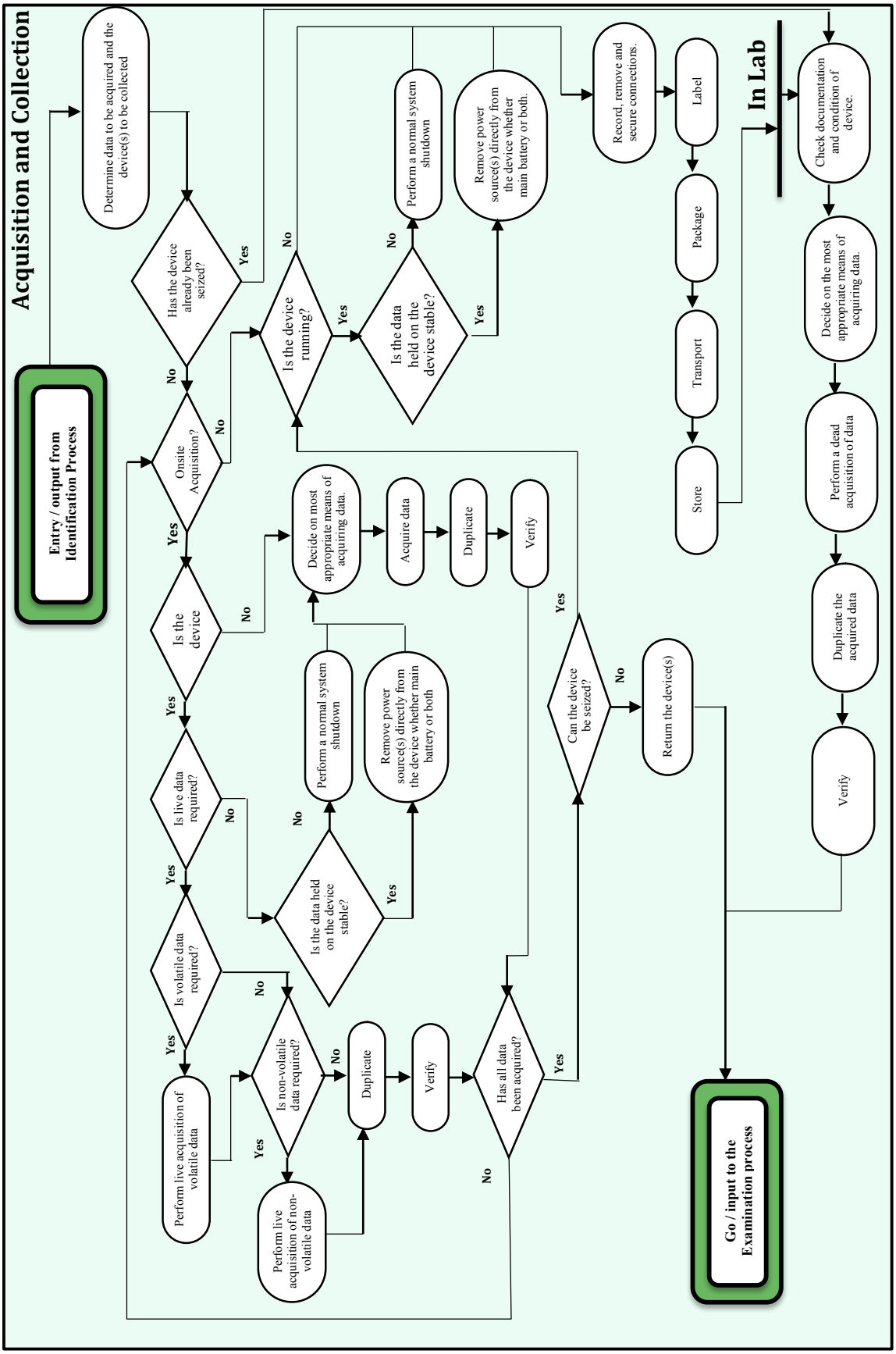


Figure 31. The UML Activity Diagram of the Acquisition and Collection Process

Laboratory Data Acquisition

In the CDFIPM, before digital evidence acquisition can be initiated, DFIs need to have already determined the data to be acquired and the digital device to be collected from the two preceding Processes. If the digital device has already been seized, phases which would need to be completed onsite if the device were not seized would become irrelevant and data acquisition will need to take place in a DFL. However, in cases where the device has not already been seized, DFIs will need to determine whether to carry out an onsite or offsite data acquisition. Various factors will influence such a decision including the type of authorisation, the type of environment in which the device is operating and also the type and size of storage media. For instance, if data resides on a mission-critical server at a hospital, it will be very unlikely that the seizure of the device would be authorised. In such circumstances, onsite acquisition would be required.

If it has been determined that onsite data acquisition is not needed and data should be acquired in a DFL[25], DFIs must then find out whether the device subject to the data acquisition is running or not. If the device is running, DFIs must determine whether the data residing on the device is stable or not before powering it down. If data residing on the device is stable, DFIs will need to remove the power source directly from the device. However, if data residing on the device is not stable, a normal shut down must be performed. In both cases where the device was running and then shut down or the device was already in powered-off state, DFIs must record, remove, secure and label the connection for the device before packaging the device for transportation back to a DFL or a secure storage. It is essential for DFIs also to collect any material which might be associated with the potential digital information. These materials can include, but are not limited to, paper containing passwords, cradles and power connectors for embedded system devices, etc. When labelling the digital device, DFIs will need to ensure that evidence labels are not placed directly on the mechanical parts of the digital media, and that they do not conceal important information such as the serial number, model number and part number.

[25] In certain circumstances, in accordance with the legal requirements, the digital evidence must be stored for a certain period of time prior to data acquisition, examination and analysis (Cohen, 2009; Ciardhuáin, 2004).

The device will then need to be transported and stored in a secure and suitable facility for subsequent laboratory data acquisition, examination and analysis. Preserving the integrity of evidence and chain of custody while the evidence is being kept in storage is of extreme importance (Montasari, 2015; Cohen 2009; Ciardhuáin, 2004). Prior to conducting the data acquisition in a DFL, the investigator assigned with this task must check the documentation and the condition of the device to ensure that it has not been damaged due to factors such as shock, temperature, pollution, loss of power and malfunction.

In order to acquire data, the investigator must then decide on the most appropriate means of acquiring data based on the Standard Operating Procedures of the organisation within which he operates as well as his own training, skills and experience. When selecting the most appropriate methods of data acquisition, DFIs should also consider the common practices suggested by ISO/IEC 27043 (2015); ISO/IEC 27037 (2012); ISO/IEC 10118-2 (2010); ACPO (2012). At all times, DFIs must be able to justify their reasons for the selection of a particular method or tool over the other methods or tools. Only those data acquisition methods that can be reproducible or verifiable by different DFIs should be selected. DFIs must perform the evidence acquisition in such a way that its integrity is preserved. This is especially important if digital evidence is intended to be used at a later stage to draw formal conclusions in a report presented to a court of law.

Therefore, the potential digital evidence must be acquired in the least intrusive manner in order to avoid altering or spoiling the evidence. In cases where the alteration to digital data is unavoidable, DFIs should document the activities performed to justify the alterations made to digital data. Depending on the type and urgency of the investigation, the CDFIPM suggests that the methods selected for data acquisition should be based on the situation, and the costs incurred and time required in order to ensure an effective digital investigation. After deciding on the most appropriate methods of acquiring data, the investigator will need to acquire the master copy of the raw data representing the potential digital evidence by creating a verifiable image of all the bits and bytes contained within the digital device. A duplicate copy of the acquired data should also be created to become the working copy in order to preserve the master copy in case it is needed to make further copies at a later stage from the master copy.

The original source and the digital evidence copies should then be verified with a proven function such as MD5 or SHA1. The hash value of both data sets must be exactly the same to ensure that the original data has not been modified. Verifying the extracted data as genuine attains legal validity (Kohn et al., 2013, Casey, 2011, Cohen, 2009). As already stated, in certain circumstances, it is not practical or permissible to acquire a digital evidence copy of the entire evidence source due to its large storage size. In such circumstances, DFIs employing the CDFIPM should perform a logical acquisition that targets only specific data types, directories or locations. Having performed data acquisition and image verification, the investigation moves to the next stage of the CDFIPM, the Examination Process (discussed later), where DFAs take over to conduct the subsequent Processes of the CDFIPM.

Onsite Data Acquisition

If it has been determined that the onsite data acquisition is required, DFIs must then decide whether the device from which the data is to be acquired is running or not. In turn, knowing the state of the device will determine whether live data acquisition should be conducted or not. If the device is not running, to acquire data, DFIs must undertake the same data acquisition steps as those described under the DFL data acquisition. The only difference would be that the static data acquisition must be performed onsite as opposed to offsite in a DFL. Similarly, if the authorisation permits for the device to be seized, the same procedures as described under DFL acquisition should be followed concerning securing, labelling, packaging, transporting and storing the evidence.

In the CDFIPM, the transportation of digital evidence acquired onsite can differ from that of the physical device described in the preceding section. As discussed, in cases where onsite data acquisition is not required, the physical device has to be transported physically to a secure location for subsequent data acquisition, examination and analysis. However, digital evidence acquired at the crime scene can be transported both physically and electronically. In cases in which digital evidence is to be transported electronically, DFIs must take special precautions such as encrypting and digitally signing data in order to preserve the integrity and chain of custody (Montasari et al., 2015). If the device is running, DFIs must determine whether live data acquisition is required or not. If live acquisition is not needed, DFIs must then follow the same procedures as described in the preceding section concerning powering down the device

and acquiring, preserving, transporting (both physically and digitally) and storing the evidence.

However, if live data acquisition is required, DFIs must determine whether to carry out live data acquisition on volatile data, non-volatile data or both. As with the static data acquisition, the acquired data from live acquisition of both volatile data and non-volatile data must be duplicated and verified using a proven function such as MD5 or SHA1. Imaging a running computer system might cause some files pertaining to the imaging application to be written to the hard drive, therefore modifying the original evidence prior to the completion of the imaging process (Casey, 2011; Brown, 2009). In such circumstances, courts would need to be reassured that whatever information was lost because of live imaging process will not contain an adequate volume of incriminating or exculpatory evidence to make a difference in arriving at a fair conclusion of the case at hand (Kessler, 2010; Kenneally and Brown, 2006).

Regardless of the static and live data acquisition performed onsite, the CDFIPM also requires DFIs to ensure that all of the required data representing potential digital evidence has been acquired. At the end of each onsite data acquisition activity, DFIs are presented with a condition, 'Has all the data been acquired?', to determine whether all the required data has been acquired or not. If all data has been acquired, DFIs can proceed with the next activity. However, if all data has not been acquired, DFIs must perform all the previous steps until they ensure that all of the required data has been acquired. After DFIs have ensured that all of the required data has been acquired, they must then determine whether the device containing the digital evidence can be seized or not based on the authorisation. If the authorisation does not permit the seizure of the device, it will need to be returned to its rightful owner. However, if the authorisation allows the seizure of the device, DFIs must then take the same steps described in preceding section to proceed with seizing the device. At this stage, the Acquisition and Collection Process of the CDFIPM has been completed and investigation moves to the Examination Process, where DFAs initiate the Examination Process of the CDFIPM in a DFL.

3.8 Investigative Processes Class

The Investigative Processes Class represents the first layer of the CDFIPM which consists of those Processes that pertain to investigating the incident or crime that has been the reason for the digital forensic investigation. As with other Classes of the CDFIPM, the Investigative Processes Class is also multi-layered containing three further lower layers including Processes, Phases and Sub-Phase. There are six processes included in the Investigative Processes Class including: Examination, Analysis, Interpretation, Event Reconstruction, Reporting, Presentation, and Investigation Closure. Figure 32 represents the UML Activity Diagram of the Investigative Class Processes in their abstract level.

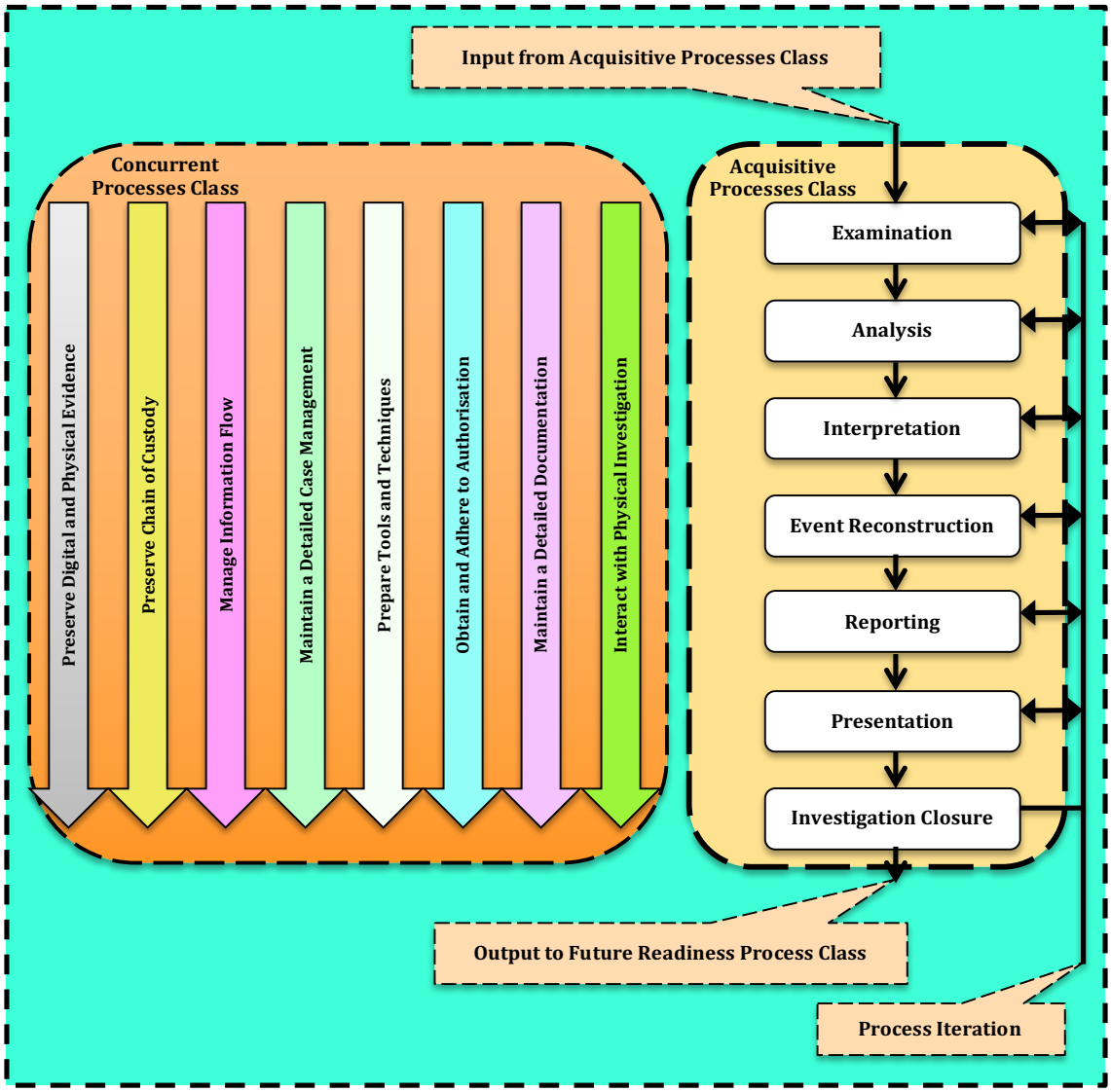


Figure 32. The UML Activity Diagram of Investigative Class Processes in their abstract level

3.8.1 Examination Process

The largest amount of investigation time is spent on the Examination Process as well as the Analysis Process (discussed later). During this Process, a large number of techniques need to be used in order to access, find and extract the acquired data representing the potential digital evidence into a human-readable format. Authors of many of the existing DFIPMs such as Carrier and Spafford (2003) state that there should be one single Phase assigned to the Examination and Analysis activities. They argue that these Phases can be confusing as their meaning is only slightly different, and it is common to have two investigators who are referring to the same tasks when they say that they are "analyzing a system" or "examining a system".

This argument is invalid on the basis that the Examination and Analysis stages have different aims and therefore should be assigned two separate Processes. The Examination Phase should involve activities regarding the extraction of potential digital evidence from the acquired data, whereas the Analysis Phase should involve those activities associated with the methodical analysis of digital evidence as well as the construction of the incident. Therefore, in the CDFIPM, the Examination and Analysis have been assigned two separate processes with their own lower-level phases and sub-phase. This approach is supported by Casey (2011), who states "Examination is the process of extracting and viewing information from the evidence and making it available for analysis", whereas "Analysis is the application of the scientific method and critical thinking to address the fundamental questions in an investigation: who, what, where, when, how, and why".

Figure 33 represents the UML Activity Diagram of the CDFIPM's Examination Process followed by the description of its lower-level components, i.e. phases and sub-phases.

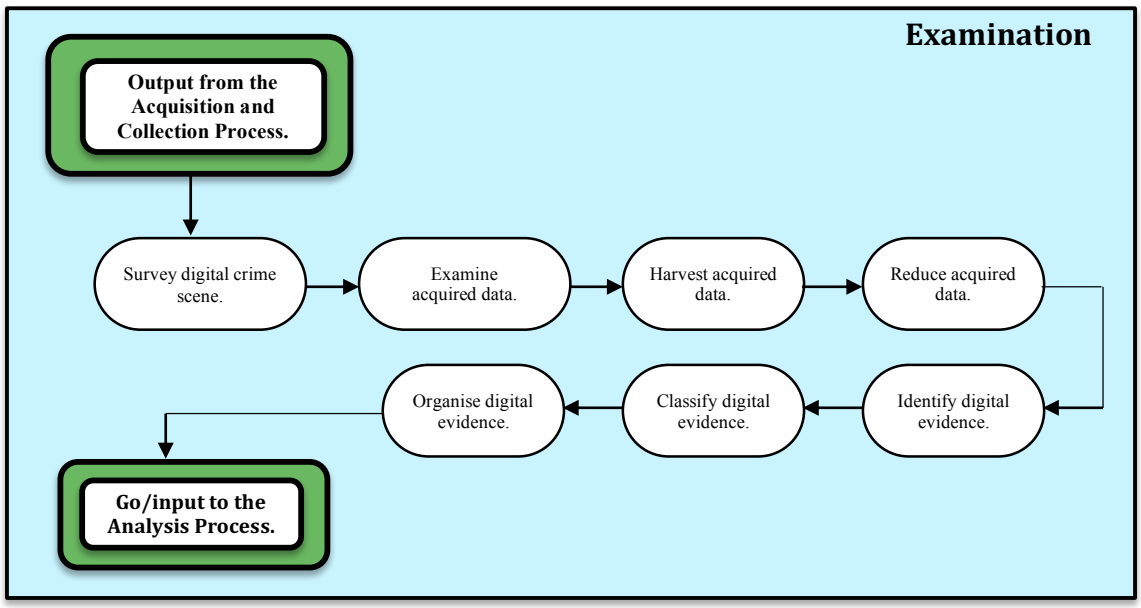


Figure 33. The UML Activity Diagram of the Examination Process

3.8.1.1 Survey Digital Crime Scene

The Survey Digital Crime Scene Phase has been developed and included in the Examination Process to enable DFAs to find apparent pieces of digital evidence for a particular category of crime in a swift manner, and also to assist them in ascertaining the skill level of the suspect. Determining the suspect's skill level in turn will allow DFAs to decide what examination and analysis techniques are required in the next process of the CDFIPM, the Analysis Process (discussed later). During the Examination Process, the first step that investigators will need to undertake is to survey the digital crime scene to identify and locate potential evidence, possibly within unconventional locations on the system (Montasari and Peltola, 2015). It is preferable to carry out the Survey Digital Crime Scene Phase in a DFL as it provides a controlled environment, and the results can be repeated with another copy of the system. To carry out this Phase in a DFL, DFAs must use the image (working copy) of the system acquired from the CDFIPM's Acquisition and Collection Process.

However, in certain circumstances, investigators employing the CDFIPM might be required to perform this phase on a live system to determine whether or not the system should be brought back to a DFL for a full examination and analysis. In such cases, investigators must perform field searches (Montasari, 2016, c; Montasari, in press) by

booting the system into what Carrier and Spafford (2003) call a "trusted environment". In cases where the Survey Digital Crime Scene Phase is to be conducted on a live system, the CDFIPM still requires the investigators to image the system so that any digital evidence could also be acquired in a controlled DFL environment. Components incorporated into the CDFIPM's Acquisition and Collection Process (see section 3.7.3) facilitate the forensic imaging of digital systems. Whether the Survey Digital Crime Scene Phase is to be carried out on a live system or in a controlled DFL environment, DFAs must adapt their investigative techniques based on the specific category of crime. This is to expedite the subsequent Examination and Analysis activities as there is often a large volume of data to deal with.

For instance, in cases where the computer has been used to store or distribute contraband images, DFAs must in the first place look for graphics with image file extensions and ascertain those that could be relied upon as incriminating evidence. Another example includes server intrusion where investigators should search for apparent signs of a rootkit installation, examine application logs and also search for new configuration files. In other types of investigations such as terrorism where investigators suspect that the system might contain the communication by the suspect, investigators must perform keyword searching to identify any leads related to the investigation. Yet another example derived from Carrier and Spafford (2003) is when analysing network traffic about an incident; the Survey Digital Crime Scene Phase might analyse traffic for the incident time frame and filter out certain ports and hosts. In other cases, as suggested by the thesis author in Montasari and Peltola (2015), the investigators should also analyse the "common" and "uncommon" locations on the system that might contain artefacts related to the suspect's browsing activities.

3.8.1.2 Examine Acquired Data

Having surveyed the digital crime scene, DFAs will need to perform a detailed examination on the image of the system (working copy) acquired from the CDFIPM's Acquisition and Collection Process. During the Examination Phase, digital evidence needs to be made visible by extracting data into a human-readable form (Montasari, 2016, c). DFAs should use the outcome of the Survey Digital Crime Scene Phase to direct their attention towards additional examination types. As an example, they will

need to conduct a keyword search once keywords are identified from other evidence. DFAs will also need to extract and process unallocated file system space for deleted files. Moreover, they should examine a low-level timeline of file activity to trace a user's activity.

Since there might be large volumes of data to be examined (Kohn et al., 2013 and Ciardhuáin, 2004), automated techniques should be employed using tools such as FTK (AccessData, 2016) or EnCase (Guidance Software, 2016) in order to support the investigators. Furthermore, a large number of techniques might be performed to process the obfuscated data such as deleted or hidden data utilising sound digital forensic methods[26], as File Allocation tables or disk indexing might be deleted in some investigations. Therefore, this Phase will enable DFAs to ensure that files such as partially deleted files are recognized from the original evidence. During this Phase, DFAs can also reverse engineer suspicious executables and examine encrypted files (Carrier and Spafford, 2003). They must also examine all the network packets that were acquired by monitoring software. In certain circumstances, it might be necessary for DFAs to examine the contents of every cluster (physical search) or every file (logical search) (Casey, 2011). They will also need to ensure that they employ different search techniques, when appropriate, when preforming this Phase.

3.8.1.3 Harvest Data

After all data including partially discovered files and folders has been made visible in the Examine Acquired Data Phase, data then needs to be harvested by giving a logical structure to the entire data set. During this Phase, the file and folder structure is indexed to provide structure to data which was acquired in the Acquisition and Collection Process of the CDFIPM. In this phase, raw data will be shown as information, and the partially deleted files which were processed during the Examine Acquired Data Phase will become visible to the degree that they were rendered visible during the Examine Acquired Data Phase. The result of the Harvest Data Phase is the production of a logical structured data set (Kohn et al., 2013) where the extracted raw data has now

[26] Providing details on specific methods is outside the scope of this thesis. It is assumed that organisations within which the DFAs operate already have their own Standard Operating Procedures associated with digital data examination which the DFAs can follow.

become structured information (Cohen, 2009). Therefore, the harvested information can now be displayed by the original file systems such as Mac OS, FAT or NTFS.

3.8.1.4 Reduce Data

The data examined and analysed in the course of a digital forensic investigation can be very large. Consequently, this data needs to be reduced to expedite the Examination Process. Identifying known elements can enable the investigators to reduce data. Investigators will need to use the metadata and unique identifiers, such as MD5, in order to remove known system files and different other application data (Casey, 2011; Cohen, 2009; Beebe et al., 2009). Data that remains will be modified data or data that could be uniquely attributed to the users of a specific computer system. Digital evidence with similar identifying patterns should also be classified based on the types of investigation.

3.8.1.5 Identify, Classify and Organise Digital Evidence

During the Identify Digital Evidence Phase, DFAs must use the known digital evidence data in order to identify the possible incident to be investigated. The outcome of this Phase will be the identification of the potential digital evidence from data that has been examined, harvested and reduced. In the Classify Digital Evidence Phase, DFAs should group together digital evidence with similar identifying pattern based on the types of investigation. This phase will enable the speeding up of the Analysis Process discussed in the next section. During the Organise Digital Evidence Phase, DFAs will need to organise digital evidence in a way so that digital forensic investigation can be accelerated. This can be materialized by focusing on the incident type identified and the data classified. DFAs should restructure digital evidence in order to conduct the identified investigation more appropriately. If similar types of incidents or crimes have taken place in the past and are known to DFAs, they should then use the known classification in order to compare the current digital forensic data (representing potential digital evidence) to the similar past incidents or crimes. At this stage, the Examination Process of the CDFIPM is completed, and its output becomes the input to the Analysis Process, discussed in the following section.

3.8.2 Analysis Process

Based upon the results of the Examination Process, DFAs must now be able to define what the exact characteristics of the incident are and who is to be held accountable for the incident. The aim of the CDFIPM's Analysis Process is to enable the investigators to reconstruct fragments of data based on their significance and to determine a possible root cause of the incident (Montasari, 2016, c; Montasari et al., 2015). The Analysis Process is the most time-consuming stage of the investigative process. Because of the volume, diversity and complexity of data to be analysed in present time digital investigations, the analysis of evidence becomes a challenge. Therefore, DFAs following the CDFIPM should use accredited automated techniques during this Process to complement manual validation techniques in order to expedite this Process. Figure 34 represents the UML Activity Diagram of the CDFIPM's Analysis Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

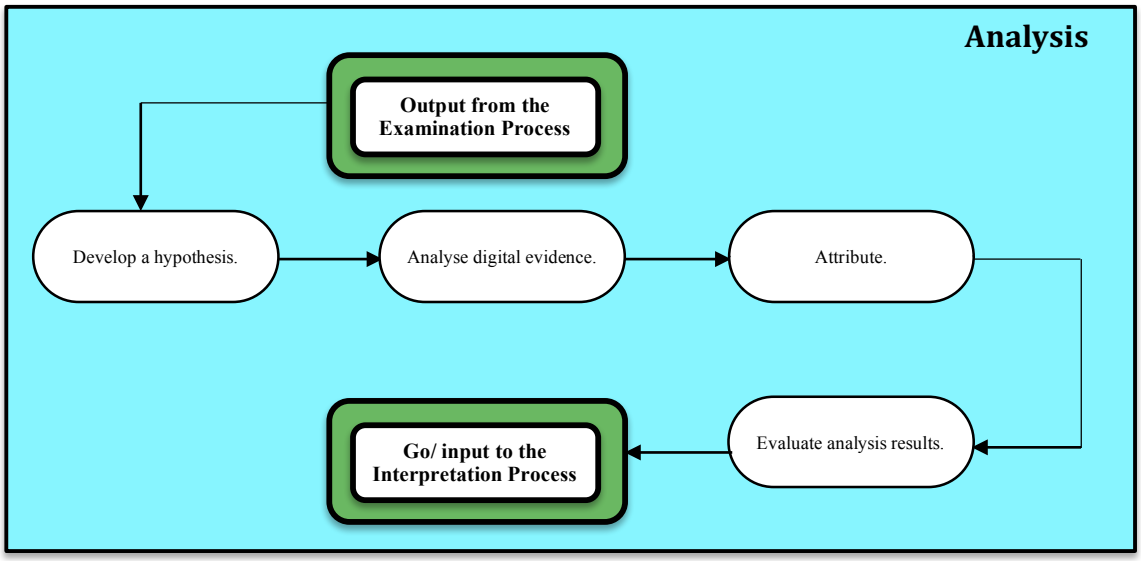


Figure 34. The UML Activity Diagram of the Analysis Process

3.8.2.1 Develop a Hypothesis

Up to this point in the investigation, DFAs have only dealt with what is possibly known from the digital evidence (Montasari et al., 2015). Now, DFAs must be able to formulate a hypothesis of how the incident took place by reconstructing a sequence of events which have resulted in the current state of the system under investigation. In

order to develop a hypothesis for the incident or crime, DFAs should base their theory on the followings:

- The assumptions that they have deduced from the phases contained in the Examination Process;
- Digital evidence that they have already organised from the Organise Digital Evidence Phase contained in the Examination Process; and
- The documentation of the crime scene that they have maintained.

3.8.2.2 Analyse Digital Evidence

After DFAs have formulated the hypothesis, they will need to perform the Analyse Digital Evidence Phase. During this Phase, DFAs must thoroughly investigate and test data that was organised in the Examination Process against the hypothesis that was formulated in the Develop a Hypothesis Phase in the Analysis Process. DFIs must also question the legal validity of the possible digital evidence by considering issues such as relevance, admissibility and weight as discussed in section 2.3.2. This will enable them to test the hypothesis by identifying the best possible evidence.

3.8.2.3 Attribute

Digital evidence should then be linked and attributed to a specific user or the event which is the root cause of the incident or crime. In order to link an individual to the incident or crime, DFAs must be able to correlate the results of the digital crime scene with physical evidence. For instance, in some investigations DFAs are likely to need to correlate data center access logs to logins, linking online chat activities found on the computer with the activity with an undercover officer, and correlating activity on a compromised server with activity on the suspect's home system and network activity recorded by an ISP.

3.8.2.4 Evaluate Analysis Results

After the attribution has been made, during the Evaluate Analysis Results Phase, the DFAs must then evaluate their findings in order to ensure that the hypothesis they have

developed holds true. Finally, in order for the Analysis Process to be most effective, DFAs might need to request other digital crime experts to assist them in correlating the event from numerous sources of digital evidence. At this stage of the Investigative Process, backtracking from the Analysis Process to the Examination Process is often to be expected as the investigators acquire a better understanding of the events which resulted in the investigation in the first place. Having completed all the Phases of the Analysis Process, this Process is now complete, and DFAs must start preparing for the interpretation of the analysis in the next process. The output of the Analysis Process will become the input to the Interpretation Process discussed in the next section.

3.8.3 Interpretation Process

The main purpose of the Interpretation Process is to use scientifically proven methods to explain facts discovered throughout the Analysis Process within the context of the investigation (Montasari, 2016, c; Palmer et al, 2001). Therefore, after investigators have evaluated their findings in the Analysis Process and have determined that the hypothesis they formulated holds true, they will need to interpret the digital evidence in order to produce meaningful statements in the legal context for later reporting and presentation.

During this Process, DFAs must be able to reconstruct the events associated with the digital investigation aspect. They should now be able to employ the results of the analysis techniques that they performed during the Analysis Process to put together the pieces of digital puzzle so that an accurate reconstruction of events can be made. Figure 35 represents the UML Activity Diagram of the CDFIPM's Interpretation Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

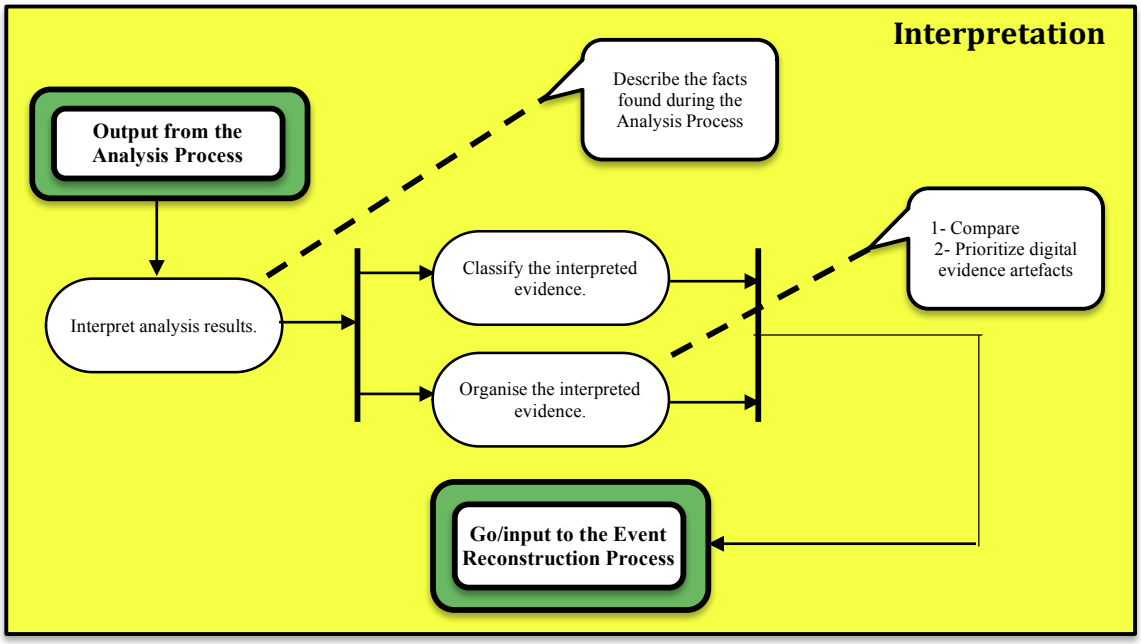


Figure 35. The UML Activity Diagram of the Interpretation Process

3.8.3.1 Interpret Analysis Results

Interpretation of any evidence should depend on the available information regarding the circumstances surrounding the creation of that item of digital evidence (Valjarevic and Venter, 2015; ISO/IEC 27043, 2015). Investigators will need to obtain information from individuals involved in the day-to-day operation of the system under investigation. This will enable them to carry out a more effective interpretation of evidence. Moreover, investigators must consider information concerning the goal as well as the scope of the investigation. In cases where the contextual information changes, investigators might also need to change the interpretation so that the interpretation can reflect any such changes regarding the contextual information. Finally, during this process, DFAs must utilise link analysis and timeline tools to enable them in the digital reconstruction (see Appendix A).

3.8.3.2 Classify and Organise the Interpreted Evidence

Having interpreted the analysis results, investigators will now need to classify and evaluate the interpreted evidence in order to ascertain the amount of trust that they can place in it. DFIs will also need to organise the interpreted digital evidence according to relevance in such a way that they can differentiate which digital evidence items are

more important than the others. DFIs following the CDFIPM should perform the Classify the Interpreted Evidence Phase and Organise the Interpreted Evidence in the Interpretation Process in parallel. This is due the fact that although both phases have different activities, they have the same aim. Finally, during the Analysis Process, DFAs will need to employ scientific methods in order to prove or refute theories based on digital evidence. After performing this process, DFAs should be able to determine how digital evidence came into existence and what its presence denotes. After completing the Interpretation Process, DFIs will need to reconstruct the events in the next process of the CDFIPM. Therefore, the output of the Interpretation Process will become the input to the Event Reconstruction Process discussed in the next section.

3.8.4 Event Reconstruction Process

In the CDFIPM, the Event Reconstruction Process and Interpretation Process are closely related in that both Processes will require DFAs to reconstruct the events associated with the digital investigation. Similar to the Interpretation Process, the Event Reconstruction Process requires DFAs to employ scientific methods in order to prove or refute theories based on the results of the analysis, and digital evidence that they have discovered. The only difference between the two Processes is that in the Event Reconstruction Process, DFIs will need to consolidate, review and test their findings against the original hypothesis that they formulated in the Analysis Process.

Having completed the Interpretation Process in the previous stage, DFAs should now be able to reconstruct a possible event sequence under the Event Reconstruction Process which reflects the incident result as accurately as possible. In order to reconstruct the events, DFIs will need to utilise the series of events that they have deduced from digital evidence which is known to them. During this Process, DFAs must ensure that they are not dealing with reconstruction as a finding based on the original digital evidence (Kohn et al., 2013). Moreover, as Kent et al. (2006) state, Event Reconstruction should not be established as factual. Instead, DFAs who perform the Event Reconstruction Process should use this Process to explain how the incident might have taken place. Figure 36 represents the UML Activity Diagram of the CDFIPM's Event Reconstruction Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

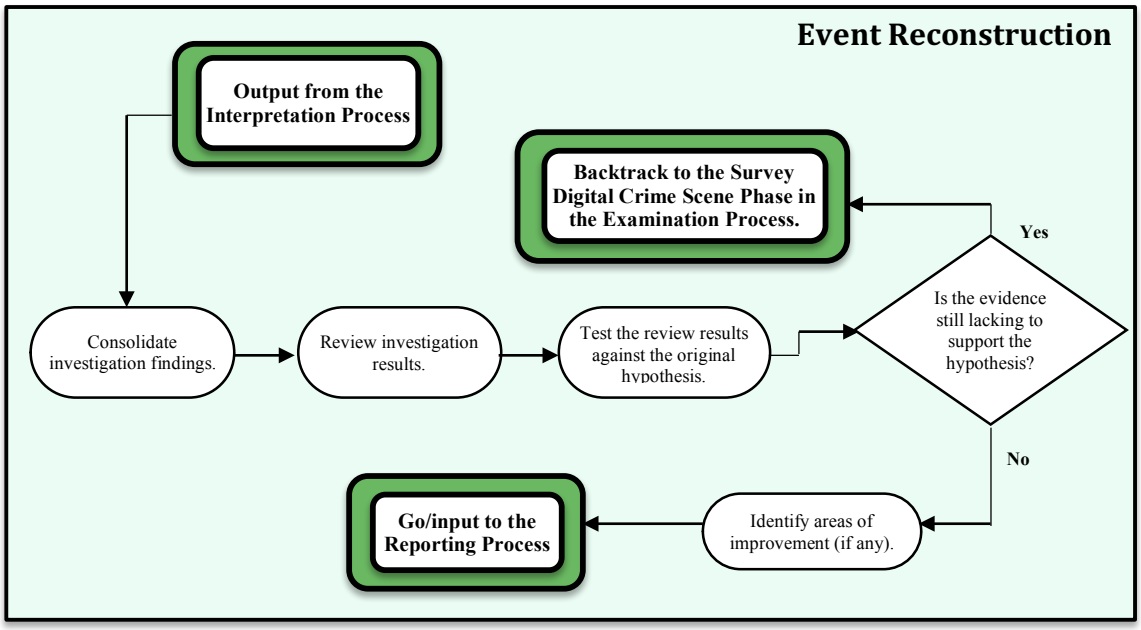


Figure 36. The UML Activity Diagram of the Event Reconstruction Process

3.8.4.1 Event Reconstruction Components

During the Event Reconstruction Process, the investigation findings must be consolidated and refined prior to assessing the review results against the original hypothesis, which was formulated in the Analysis Process. This will be to determine whether DFAs have acquired all the evidence required to support the original hypothesis. If all the evidence has not been captured, DFAs will need to backtrack to the Survey Digital Crime Scene Phase in the Examination Process, in which this Phase and subsequent Phases form a cycle that needs to be repeated until DFAs can identify additional evidence and explain the incident.

As an example, in cases where a server intrusion has taken place, this iteration would involve DFIs linking the exploitation of a service that is open to attack with the installation of a rootkit and utilization of a network sniffer. The source IP address of network connections could result in the acquisition of additional digital evidence to examine. If there is no need to iterate to the Examination Process at this stage, DFAs must identify any areas of improvement and address those required improvements. In order to press charges against the perpetrator and explain the incident in a court, DFAs must have a valid hypothesis accompanied by relevant admissible digital evidence to support the findings that they have deduced. Finally, during the Event Reconstruction

Process, DFAs might benefit from using link analysis and timeline tools to assist them in the digital reconstruction. The Event Reconstruction Process of the CDFIPM is completed at this stage and DFAs should prepare for the next Process where they will need to compile a report to be presented in a court or the management in a company. The output of the Event Reconstruction Process will become the input to the Reporting Process, discussed in the next section.

3.8.5 Reporting Process

After conducting the Event Reconstruction Process, DFAs will need to compile, write and print out on paper a detailed and concise report in the Reporting Process. Regardless of digital evidence or physical evidence, a forensic report must contain conclusions that can be reproduced by independent third parties. Forensic reports that include opinions based on accurately documented digital sources are much more likely to withstand judicial scrutiny than opinions based on less reliable sources (Garrie, 2014). DFAs following the CDFIPM must detail in their report all the findings and results of the entire digital investigative process including the Concurrent Processes (Overriding Principles) of the CDFIPM such as documentation, chain of custody, digital evidence preservation, authorisation and management, and ultimately the investigators' findings that are constructed in an opinion to be presented in a court.

In addition, the forensic report should follow "the 'ABC's of writing' (accuracy, brevity, and clarity)" and be restricted only to what is known (Beebe and Clark, 2005). DFAs will need to write their report in such a manner that it contains conclusions that can be reproduced by independent third parties regardless of digital or physical evidence. Also, since digital forensic investigation might produce many incriminating digital evidence items, DFAs must therefore ensure that they list all digital evidence items in the report so that no valuable item of evidence is left out. Furthermore, DFAs must ensure that they include in the report all other relevant documentation that was compiled during the investigation and that might be relevant in reaching a decision. Figure 37 represents the UML Activity Diagram of the CDFIPM's Reporting Process.

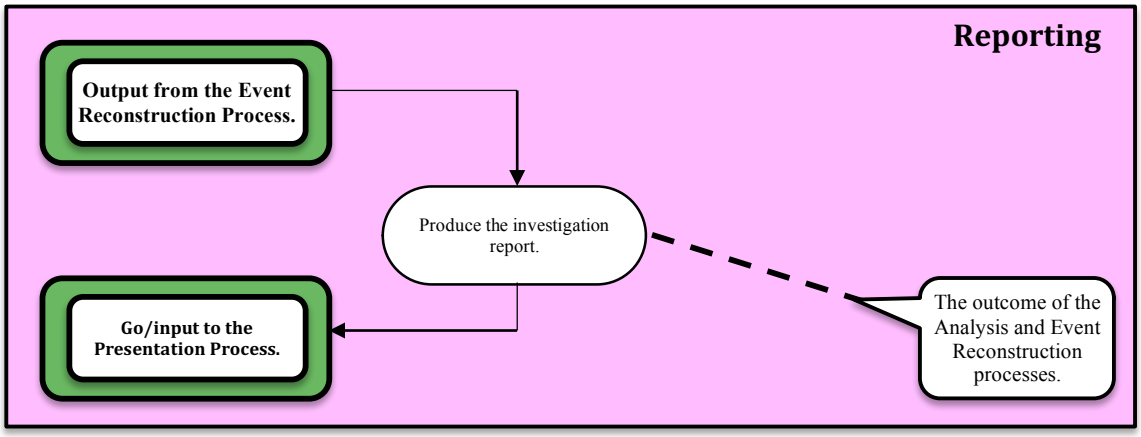


Figure 37. The UML Activity Diagram of the Reporting Process

DFAs should also ensure that they reference accepted and known protocols and methods applied during the Examination, Analysis, Interpretation and Event Reconstruction Processes in order to increase the credibility of the investigation and its results. Finally, DFAs employing the CDFIPM must ensure that their report is in a simple language and is well-defined, concise and unambiguous in order for the lay person to be able to understand it. After DFIs have compiled the report and are satisfied with its content, the report will then need to be presented in a court. The output of the Reporting Process becomes the input to the Presentation Process of the CDFIPM, discussed in the next section.

Notice: See Appendix A for an example of a forensic report in which the activities performed throughout a hypothetical digital forensic investigation are explained to a hypothetical court of law. This hypothetical digital investigation, presented in the Appendix A, has been carried out along with the use of case studies, presented in Chapter 4, to demonstrate the application of the CDFIPM.

3.8.6 Presentation Process

The output of the Reporting Process in the form of a well-written report must be presented to a wide variety of audiences such as courts, legal personnel, law enforcement, technical personnel and management. Presenting the report can be carried out in the form of the expert report or can be accompanied by other formats such as multimedia presentation, deposition and expert witness (testimony). During the

Presentation Process, DFAs will need to be able to prove the hypothesis that they formulated during the Analysis Process using supporting evidence. In order to prove that all of the CDFIPM's previous Processes were conducted accurately, evidence that DFAs present must hold up in a court.

Although Presentation Process is very important in that it meets the main requirement needed by the definition of the word 'forensic', authors of the existing models have paid little attention, if any, to this Process. Researchers have often taken a cursory approach when dealing with the Presentation Process and have often confused this Process with the Reporting Process. In the existing models, Presentation Process and Reporting Process are regarded the same, and as a result they are assigned one single process under the naming either "Report" or "Presentation". This approach is flawed on the basis that the Reporting Process and Presentation Process are carried out at different times and under different circumstances during the course of an investigative process and as a result have different aims. The purpose of the Reporting Process should be to document relevant information deduced from the findings and results of the investigative process, whereas the aim of the Presentation Process should be to communicate such information and findings to the said audience. Therefore, in the CDFIPM, the Presentation Process has been distinguished from the Reporting Process, and as a result each has been assigned a separate and discrete Process in the model.

Moreover, the "Report/Presentation" in the existing models is often a high-level Process without providing adequate details to assist DFAs in effectively preparing for this important Process. Since careful planning is essential especially when the investigation findings are to be presented in a court, the Presentation Process of the CDFIPM has incorporated lower-level and generic phases to guide the DFIs on how to prepare for this Process.

During the Presentation Process, DFAs must communicate their findings in such a way that facilitates future validation and that can be understood by both technical and non-technical audience. Mumba and Venter (2014) state that during the Presentation Process, it is vital that all of the processes are utilised to prove that the investigation was conducted in a forensically sound manner. Beebe and Clark (2005) highlight that a presentation should be based on "careful consideration about how to best communicate

information to various audiences". Therefore, during the Presentation Process, DFAs following the CDFIPM must provide both concise and detailed confirmatory information obtained from the Interpretation and Event Reconstruction Processes of the model concerning the data examined and analysed in the Examination and Analysis Processes of the model. The presentation must also include relevant documentation and processes conducted during the investigative process, as well as any relevant physical evidence that can further consolidate the case against the perpetrator. Figure 38 represents the UML Activity Diagram of the CDFIPM's Presentation Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

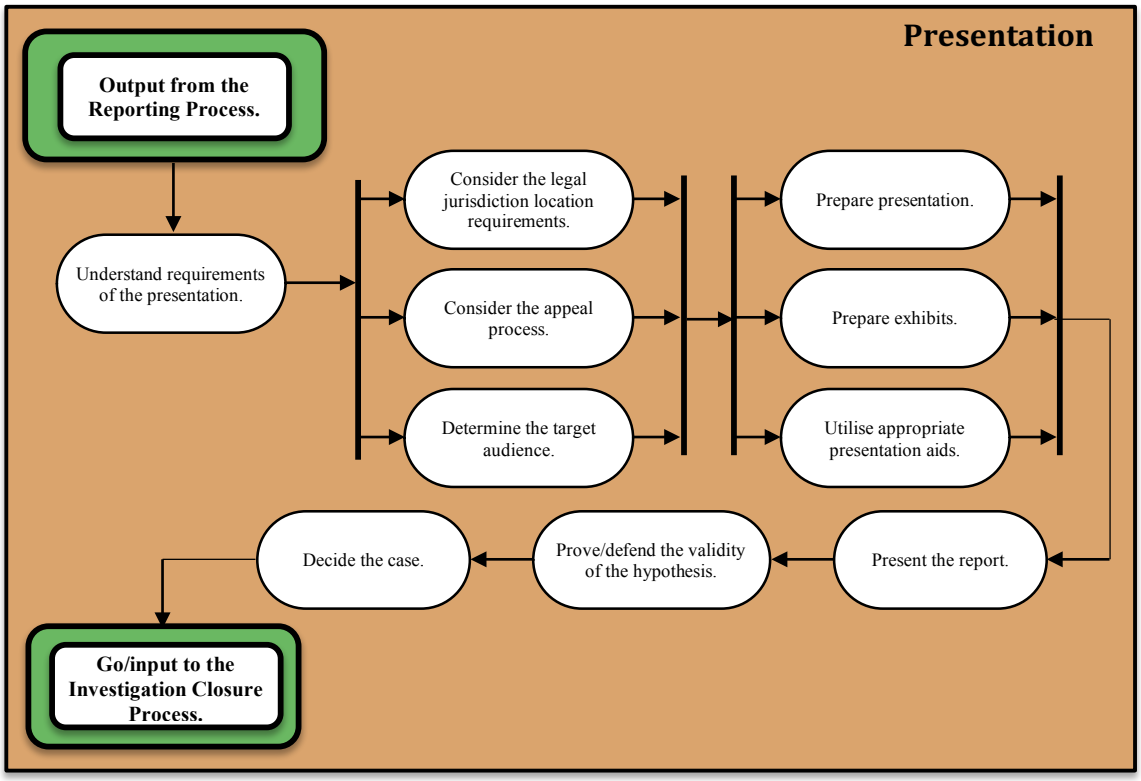


Figure 38. The UML Activity Diagram of the Presentation Process

3.8.6.1 Components of the Presentation Process

Prior to delivering the presentation, DFAs must address the following four issues:

- choosing their main points carefully based on the results of the CDFIPM's Interpretation and Event Reconstruction Processes;
- selecting their supporting information;

- developing a conclusion; and
- reviewing their presentation prior to its delivery.

Since the judge and jury or other interested parties are very likely to be non-technical users, DFAs must ensure that in their presentation they avoid complex arguments, unless providing the audience with significant help so that they understand the technical points made. DFAs must deliver their conclusion in a logical and structured manner and build upon their previous points. In addition to preparing the presentation itself, DFAs will also need to prepare supporting information in order to assist the audience in better understanding the points they make. This should include the factual data itself that they have deduced from Interpretation and Event Reconstruction Processes and also the explanation of the process. DFAs might also need to use diagrams, pictures and video if it enables the audience to understand the explained concepts more clearly. Another important stage in the Presentation Process is the conclusion that DFAs have arrived at. They must ensure that they remind the audience of their main points and leave the audience with a clear understanding of them and their judgments on the case.

After preparing the presentation and prior to appearing before the relevant audience, DFAs will need to review their presentation to ensure that its content meets the objectives of the report, is logically structured and contains the material at the right level for the audience. In cases where DFAs will have to appear before judge and jury to give expert witness, they must ensure that they are fully aware of the jurisdiction legal requirements (the U.K. in the context of this research) concerning the digital evidence. Not being aware of the legal requirements might render the incriminating evidence being thrown out of the court. Moreover, DFAs must find out in advance what legal proceedings will concern the appeal process so that they can be better prepared in case they might need to reappear before the court. Often the person who presents the findings of the case is not often involved in various stages of the investigative process such as Acquisition, Examination, Analysis, Interpretation and Event Reconstruction Processes. Therefore, DFA who is required to appear before a court as an expert witness must determine who his target audience are prior to preparing the presentation if this is not already known.

Investigators also need to ensure that they identify the exhibits (i.e. digital evidence) by a label or other mark. The exhibit must also be properly described in the report as discussed in the Reporting Process section. When delivering the presentation, DFAs must take into account that the target audience are often non-technical and might have a variety of experiences and level of knowledge concerning the digital investigations. Therefore, in order to help the audience to understand the explained concepts better while giving the presentation, DFA might need to link their investigation findings to the things that the audience already understand. DFAs need to ensure that they have targeted their findings at the right level for the needs of the audience. They must also avoid using technical jargon and should attempt to explain the abstract concepts with clear practical examples.

During the presentation, often the hypothesis[27] is challenged by the defence lawyers. A contradicting hypothesis and supporting evidence are placed before judge and jury. DFAs will need to prove the credibility of their hypothesis and to be well-prepared to defend the hypothesis against criticism and challenge. In circumstances in which challenges are successful, investigators will need to backtrack to the earlier stages to obtain and examine more evidence and develop a better hypothesis. The case will be decided based on the presentation report. If the decision is made in a court, it will be decided whether to convict the accused or whether to refute the allegations. If the decision is made in the context of an organisation, it will be decided what disciplinary actions must be taken if the incident can be attributed to the individual under investigation. At this stage, the Presentation Process of the CDFIPM is concluded, and its output becomes the input to the Investigation Closure Process, discussed in the following section.

3.8.7 Investigation Closure Process

It is vital not only to close the investigation and apply the decisions associated with it but also to maintain the knowledge obtained to improve subsequent investigations (Beebe and Clark, 2005). As the title suggests, the Investigation Closure Process of the

[27] The hypothesis must be presented to persons other than the investigators. For a police investigation, the hypothesis will be placed before a jury, while an internal company investigation will place the hypothesis before management for a decision on action to be taken.

CDFIPM involves concluding the investigation and also the decision-making on the credibility of the hypothesis presented in the Presentation Process. This denotes that after completing the Investigation Closure Process, investigators can backtrack to any of the preceding processes that follow the First Response Process. Figure 39 represents the UML Activity Diagram of the CDFIPM's Investigation Closure Process followed by the description of its lower-level components, i.e. Phases and Sub-Phases.

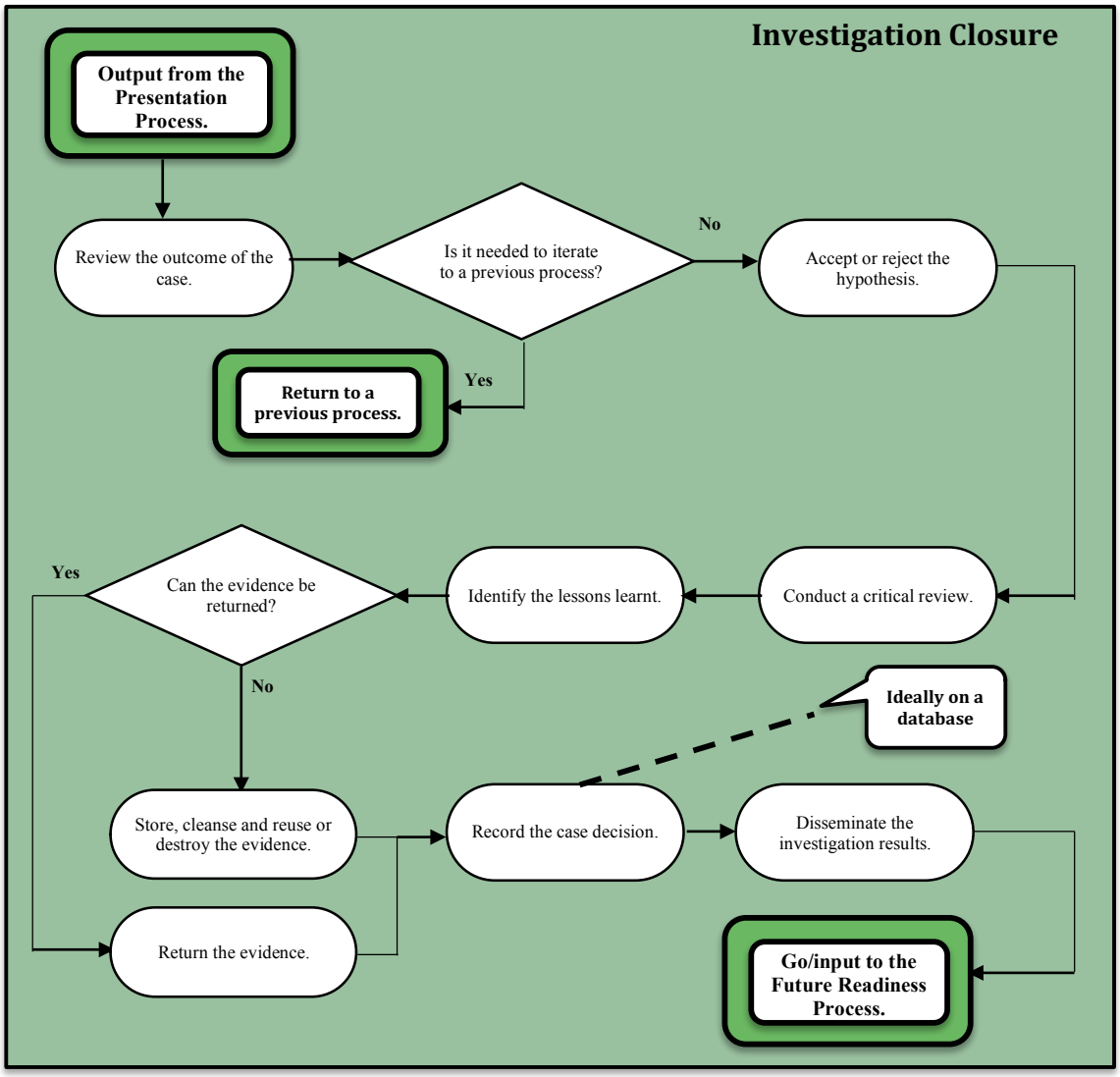


Figure 39. The UML Activity Diagram of the Investigation Closure Process

3.8.7.1 Review the Outcome of the Case

After the case has been presented to the appropriate audience and decided in the Presentation Process, the outcome of the investigation will need to be used to review the existing policies and procedures of the organisation. The aim of this Phase should be to

make and act upon the outcome of the decisions reached from the CDFIPM's Presentation Process. During this Phase, the investigating organisation will also need to collect and maintain all the information associated with the case that has been investigated.

3.8.7.2 Accept or Reject the Hypothesis

Since the CDFIPM is an iterative process model, it will allow investigators to backtrack to any of the preceding Processes in the model. Having carried out the initial review, at this stage the investigators can return to any of the CDFIPM's previous Processes that follow the First Response Process if required.

3.8.7.3 Conduct a Critical Review

During the Conduct a Critical Review Phase, the entire investigative process detailed in the CDFIPM must be reviewed to identify any lessons learnt and potential areas of improvement. During this Phase, the investigating organisation will also need to address issues such as what went well, what did not go well and how things could have been carried out better, etc. Based on this information, the investigating organisation will need to identify and learn the lessons from the incident or crime in order to be able to apply the findings and be better prepared for the future incidents or crimes. Also under this phase, the outcomes and their ensuing interpretation must be used for refining the Acquisition, Examination, Analysis, Interpretation and Event Reconstruction of digital evidence in future investigations. As already stated, often backtracking between Examination, Analysis, Interpretation and Event Reconstruction Processes are to be expected in order to obtain the full picture of the incident or crime. Such information could also assist law enforcements' HTCUs and corporates in establishing more effective policies and procedures.

3.8.7.4 Evidence Management

A decision will also need to be made to determine whether digital and physical evidence should be returned to the proper owner or not and to determine what criminal evidence must be removed. This is a complicated issue and not an explicit step in a digital

forensic investigation. However, any of the existing models that has emphasized the seizure of evidence has seldom addressed this aspect. Jurisdiction in which the investigation is taking place (in the context of this thesis, the U.K.) and the type of authorisation determine whether the evidence should be returned, cleansed and reused or destroyed or whether the evidence should be stored for a certain period of time before any of the three possibilities can be applied.

3.8.7.5 Record the Case Decision

Under the Record the Case Decision Phase, DFIs will need to record (ideally on a database) the investigation results, case decision as well as all the evidence that might be used for reference in the future and for training purposes. For instance, the results could be recorded by the category of evidence found as follows:

- Evidence of refutation or defence;
- Evidence vital to the case;
- Evidence important to the case;
- Evidence that supports other evidence;
- Evidence peripheral to the case;
- Evidence that is intelligence only; and
- No evidence found.

Such an approach could also benefit authorities in other jurisdictions in circumstances in which the case will be likely to have some kind of connection with their investigation.

3.8.7.6 Disseminate the Investigation Results

In the final part of the Investigation Closure Process, relevant information concerning the entire investigation will need to be disseminated and communicated to all stakeholders. This includes communicating the need to return to a previous Process, deciding on the acceptance or rejection of the hypothesis or providing any reports or documents from the Presentation Process. During this Phase, the investigating organisation might decide to make some information available only within the

organisation, whereas they might decide to disseminate other information more widely. According to Ciardhuáin (2004), the investigating organisation's policies and procedures should determine the details in this regard. The information will have an impact on future investigations and might have an effect on the policies and procedures.

Thus, the accumulation and preservation of this information is a key part of supporting the work of investigators and might be a productive aspect for the development of innovative applications that integrate techniques such as data mining and expert systems. Hauck et al. (2002) provide a detailed example of the dissemination activity where they define a system titled Coplink, that provides real-time support for law enforcement DFIs through an analysis application on the basis of a large accumulation of information from past investigations. An additional example is provided by Harrison et al. (2002), whose system is not real-time, but instead delivers an "archival function" database to support investigators. At this stage, the Investigation Closure Process of the CDFIPM is concluded, and its output becomes the input to the Future Readiness Process Class, discussed in the following section.

3.9 Future Readiness Process Class

The aim of the Future Readiness Process Class is to enable both the investigating organisation and victim organisation to prepare for and mitigate the risks of potential future incidents. This class is optional; however, implementing it could increase the efficiency of the said organisations. Figure 40 represents the UML Activity Diagram of this class.

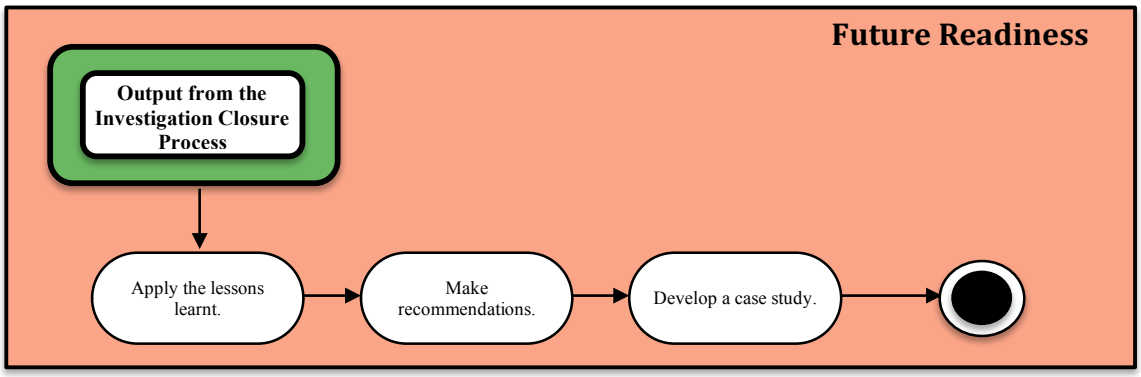


Figure 40. The UML Activity Diagram of the Future Readiness Process Class

The Future Readiness Process Class involves investigating and victim organisations applying the lessons learnt and also improving their existing policies and procedures based on the critical review of the entire investigative process performed in the Investigation Closure Process. During this Class, case studies should also be developed for future reference to enable both investigating organisations as well as the victim organisations to learn from the incident which has been investigated.

3.10 Overriding Principles

In order to ensure the admissibility of digital evidence in courts, a set of eight Overriding Principles or Concurrent Processes have also been developed and grouped into a unique class, entitled Concurrent Processes Class (see Figure 15). These eight Principles are objectives that need to be achieved in a given digital investigation and should be performed concurrently throughout the whole or parts of the other Processes in the CDFIPM. The inclusion of the proposed Overriding Principles or Concurrent Processes is justified by their significance and applicability to other digital investigation processes. Thus, due to their extreme importance, investigators must maintain these Principles at all times throughout the whole or parts of the digital investigative process. Since the CDFIPM is aimed at the U.K. jurisdiction, the proposed Overriding Principles are based on the following standards: ISO/IEC 27043 (2015), ISO/IEC 27037 (2012) and ACPO (2012), as well as other relevant scientific papers such as Montasari (2016, c), Montasari et al. (2015), Valjarevic and Venter (2015), Casey (2011), Beebe and Clark (2005), Ciardhuáin (2004) and Carrier and Spafford (2003).

3.10.1 Preserve Digital and Physical Evidence

Preservation is the process to maintain and safeguard the integrity and original condition of both physical and digital evidence. In order for evidence to be able to withstand scrutiny in courts, investigating organisations will need to prove that both digital device and digital evidence that they have handled during an investigation have not been altered, or justify their actions if unavoidable changes were made. In the best-case scenario, there should be no contamination to data itself or any metadata associated with it (e.g. date and time-stamps).

In some cases, the confidentiality of digital evidence is a requirement, either a business requirement or a legal requirement (see Section 2.3.2). This denotes that digital evidence should be preserved in a manner that ensures the confidentiality of data. Thus, since the correct handling of evidence is essential in any digital investigation (Montasari, 2010, c; Montasari, in press; Valjarevic and Venter, 2015; ACPO, 2012; ISO/IEC 27037, 2012; Holder et al., 2009), this Overriding Principle or Action Principle has been incorporated into the CDFIPM to enable investigating organisations to preserve the integrity of both digital and physical evidence throughout the entire investigative process in a forensically sound manner. Preserving this Overriding Principle will enable investigating organisations to protect both physical and digital evidence from being tampered with, contaminated or altered and as a result to ensure the efficacy of evidence presented to a court.

Almost all the existing models have undertaken a flawed approach towards the issue of preservation and have provided a superficial discussion of this aspect of digital investigative process by simply stating that digital evidence needs to be preserved without elaborating on this important aspect. Moreover, preservation in some existing DFIPMs refer only to preservation of physical evidence or crime scene (Casey, 2011; Carrier and Spafford, 2003) while in some other models it refers to preservation of only digital evidence (Kohn et al., 2013; Carrier and Spafford, 2003; Reith et al., 2002), or digital evidence during the transportation or storage (Valjarevic and Venter, 2015; Ciardhuáin, 2004; Reith et al., 2002).

Although some existing models (Casey, 2011; Carrier and Spafford, 2003) have discussed preservation in more depth, their approach of dealing with this principle is still flawed as the "preservation activity" in these models is restricted to a 'single Phase' at a particular stage of the investigative process. It is however argued that preservation has a much wider scope beyond being limited to a single point in time. Each stage of investigative process requires digital and physical evidence to be preserved in a different manner. In order to address the stated issues, in the CDFIPM, preservation has been introduced as an Overriding Principle or Actionable Principle that should be applied concurrently throughout the entire investigative processes of the model from the time the incident is detected in the Incident Detection Process up to and including the time when the investigation is formally completed in the Investigation Closure Process.

Preservation does not need to be applied during the Readiness and Future Readiness Processes on the basis that evidence (both physical and digital) is not handled during these two Processes. The remainder of this section provides some practical examples of how the investigating organisations should apply the preservation aspect of the investigative process throughout the entire stages of the CDFIPM.

During the CDFIPM's Secure and Evaluate the Crime Scene Process, the preservation might involve investigators preventing unauthorised people from entering or leaving the crime scene, isolating the system from the network, acquiring the volatile data that would be lost after the system is powered down, and detecting suspicious processes that are running on the system, etc. During the Acquisition and Collection Process, preservation involves DFIs securing log files in case that they are lost before the system is imaged. Preservation also requires DFIs to make a full forensic image backup[28] of the system so that it can be examined and analysed at a later stage in a DFL. DFIs must note that a full forensic image of the system preserves the whole digital crime scene whereas copies that are system backups preserve only the allocated data within the digital crime scene. Moreover, in terms of preserving the state of the network, this can be achieved by network monitors when they save network traffic.

Finally, as part of preservation, investigating organisations will also need to establish and maintain certain strict procedures (Valjarevic and Venter, 2015), effective quality systems such as Standard Operating Procedures (SOPs) (Bulbul et al., 2013) or procedural workflows (Mukasey et al., 2008).

3.10.2 Preserve Chain of Custody

The processes for documenting, collecting and protecting both physical and digital evidence are called the establishing of the chain of custody. Establishing a chain of custody during the course of an investigation is of extreme importance since digital evidence is very likely to be handled by various parties. Cases where Chain of Custody has not been properly preserved have been easily challenged in courts and rejected

[28] Depending on the type of crime and authorisation, a critical system can be rebuilt after investigators have created a forensic image in order that it can be swiftly placed back online (Carrier and Spafford, 2003). In contrast, in other circumstances, the original hard disk must remain as physical evidence during the entire duration of the case.

irrespective of evidence discovered from the suspect's computer system. Therefore, due to its extreme importance in relation to conducting a successful investigation, Chain of Custody has been incorporated into the CDFIPM as an Overriding Principle, namely Preserve Chain of Custody, that will need to be applied concurrently throughout other Processes of the CDFIPM. In order to preserve Chain of Custody, DFIs will need to adhere to all legal requirements and must document each given process of the CDFIPM thoroughly. Documentation (discussed later) is a vital aspect of a Chain of Custody as it will need to detail the activities associated with the chronology of the movement and handling of evidence such as those associated with the seizure, custody, control, transfer, examination, analysis and disposition of both physical and digital evidence.

The issue of establishing Chain of Custody has been ignored by almost all the existing models, a problem identified also by Kohn et al. (2013), Ciardhuáin (2004) and Carrier and Spafford (2003). Although Chain of Custody has been addressed to some extent by four guidelines and standards including: ACPO (2012), ISO/IEC 27037 (2012), ISO/IEC 27035 (2015) and ISO/IEC 27043 (2015), these appear to be contradictory in terms of the point at which Chain of Custody will need to be established during an investigative process. For example, according to ISO/IEC 27037 (2012) and ACPO (2012), Chain of Custody should be initiated from the Acquisition Process onwards, whereas ISO/IEC 27043 (2015) and ISO/IEC 27035 (2015) state that Chain of Custody must be maintained throughout the entire investigative process.

The approach taken by ISO/IEC 27037 (2012) and ACPO (2012) is flawed on the basis that digital device containing potential digital evidence is identified in the incident detection stage prior to the Acquisition Process. It is in the Incident Detection stage that the investigating organisations will need to process both physical (where items of evidentiary value exist) and digital crime scenes and therefore initiate the chain of custody. Consequently, in line with ISO/IEC 27043 (2015) and ISO/IEC 27035 (2015), DFIs following the CDFIPM must observe this Overriding Principle from the Incident Detection Process, during which incident is detected, up to and including the Investigation Closure Process, where incident is formally closed.

One of the benefits of such an approach taken by the thesis author is that it will enable DFIs to trace back the history of any digital device containing evidence to the time that

it was first identified until its present status and location. Another benefit of this approach is the enabling of the identification of access and movement of potential digital evidence at any given point in time.

In any type of investigation, investigators within the investigating organisations are often accountable for all the acquired evidence (both physical and digital) during the period in which evidence is within their custody. The CDFIPM's Preserve Chain of Custody Principle also requires DFIs to keep records of who was responsible for handling both physical and digital evidence. Investigators must keep a record of all information associated with different activities undertaken in relation to Chain of Custody. The Chain of Custody record itself may comprise more than one document and include a series of related documents. For instance, for potential digital evidence, there should be a contemporaneous document recording the acquisition of digital data to a particular device, the movement of that device and documentation recording subsequent extracts or copies of potential digital evidence for analysis or other purposes.

An example of preserving Chain of Custody is when evidence copies are required to be shared with other experts in other locations. This handling of evidence must be properly documented to preserve Chain of Custody. Another example of Chain of Custody is when the first responders (who are the first custodian to preserve Chain of Custody of potential digital evidence) arrive at the crime scene where they will need to describe the scene in the preliminary drafting of documentation. These include taking photographs, videos and sketches.

The CDFIPM's Preserve Chain of Custody Principle does not impose any particular format in which information related to Chain of Custody should be recorded. The documents detailing Chain of Custody can be in the form of digital data or other formats such as paper notes, depending on the organisation or the agency conducting the investigation. The CDFIPM's flexibility allows investigating organisations to design and incorporate into the model their own Chain of Custody forms according to their needs. A Chain of Custody form that has been designed and used as part of a hypothetical digital investigation is still provided in Appendix A that investigating organisations can employ.

3.10.3 Manage Information Flow

One of the major issues with the existing models is the lack of identifying 'Information Flow' which could have a negative impact on the other processes such as Chain of Custody. In this regard, Ciardhuáin (2004) criticizes the past models stating, "The single largest gap in the existing models is that they do not explicitly identify the information flows in investigations." Ciardhuáin (2004) proceeds to propose what would become one of the most widely referenced research papers in relation to Information Flow within a digital investigation. In his research paper, Ciardhuáin (2004) is able to define, identify and describe Information Flows within his process model so that its stages can be protected and supported technologically. Moreover, he clearly shows Information Flow that must exist amongst various stakeholders.

Due to the fact that the subject of Information Flow within the field of digital forensics has been extensively covered by the aforementioned reference, this thesis does not aim to focus on Information Flow in any further detail. However, due to its importance in a digital investigation, Information Flow has been incorporated into the CDFIPM as an Overriding Principle, namely Manage Information Flow, which needs to be managed concurrently throughout the entire processes of the CDFIPM. Investigating organisations employing the CDFIPM must manage Information Flow from the Readiness Process up to and including the Future Readiness Process. The rationale for including this principle in the CDFIPM is to enable investigating organisations to deal with the different laws, practices, languages, etc. correctly in digital investigations. An example of Information Flow could be the interaction between two investigators involved in the same investigation, or the exchange of digital evidence between various parties during digital investigation process. Information Flow can be protected, for instance, by utilising trusted public key infrastructure (PKI) and time stamping to identify the different investigators and authenticate evidence in addition to protecting the confidentiality of the evidence through PKI-based encryption.

3.10.4 Maintain a Detailed Case Management

As the title suggests, Case Management refers to managing the case under investigation and keeping track of evidence items, events and vital forensic discoveries. Case

Management mainly pertains to the tasks that a case officer should undertake throughout the entire investigative process in an investigation, and also to some extent relates to the responsibilities of the case officer's investigative team members. Activities associated with the Case Management can have significant impact on the entire investigative process tying together all of the activities and their outcomes. Casey (2011) highlights the importance of the Case Management stating, "Effective case management is one of the most important components of scaffolding, helping digital investigators bind everything together into a strong case." Similarly, Khatir et al. (2008) proclaim that the effectiveness of a digital investigation is reliant upon Case Management.

The lack of effective Case Management methods will result in investigative opportunities being easily neglected, digital evidence being disregarded or lost, and incriminating information representing potential digital evidence remaining undiscovered or not being passed onto decision makers. Therefore, due to its importance in a digital investigation, Case Management has been incorporated into the CDFIPM as an Overriding Principle, namely Maintain a Detailed Case Management, that will need to be applied from the Readiness Process up to and including Investigation Closure Process. The rationale for including this principle into the CDFIPM is as follow:

- to outline the responsibilities and certain important tasks that both a case officer and his investigative team members will need to undertake in order to ensure a successful investigation (Khatir, et al., 2008);
- to enable a smooth transition between different Processes of the model; and
- also to ensure that all applicable information that results from each Process is acquired, documented and intertwined together in order to reconstruct the events associated with the crime or incident in a vivid and compelling manner.

The remainder of this section provides some examples of the tasks and types of responsibilities that a case officer and his investigative team members are to undertake under this Overriding Principle, Maintain a Detailed Case Management.

The tasks of a case officer start after the incident has been reported in the Incident Detection Process, where he needs to decide whether to accept or reject the case and determine the time and budget required to carry out the investigation. The case officer will subsequently need to develop an accurate and detailed plan that investigators can follow; this plan must define clearly the milestones, goals and sub-goals within the investigative process (Khatir, et al., 2008). The case officer must also allocate tasks to individual team members[29], oversee these tasks as well as drawing a complete picture of the entire investigative process and its outcomes so that the investigation does not deviate from its correct course. In circumstances where the investigation has deviated from its correct course, the manager will need to identify the root cause of the deviation and guide the team members into the correct path. Case officers will also be responsible for obtaining written authorisation so that the investigation can proceed as well as determining what level of attention to give to a particular case comparative to all of the other cases that they are dealing with (Khatir et al., 2008).

As already stated, in addition to the case officers, the Maintain a Detailed Case Management Principle also pertains to the investigative team members who will need to undertake various tasks under this Overriding Principle. These include communication and prioritization such as sharing information amongst DFIs, meeting the requirements of non-technical stakeholders, prioritizing and assigning administrative tasks amongst multiple DFIs in a digital investigation, etc. In certain investigations, communication becomes a key aspect of case management (Khatir et al., 2008). For example, in complex investigations that might last for long time, daily or weekly status meetings are required in order to discuss and analyse progress, combine up-to-date information and discuss and review the following steps in the investigation. Finally, logging digital evidence in archives is another important factor in managing an investigation effectively. This task can be carried out by both the case officer or the investigative team members (Khatir et al., 2008).

[29] The team setup is required due to the fact that different stages of the investigative process require a diverse set of investigators with different expertise such as digital forensic examiners, first responders, digital forensic practitioners, digital forensic examiners and digital forensic analysts.

3.10.5 Prepare and Test Tools and Techniques

It is vital that DFIs prepare an appropriate set of tools and techniques during the course of an investigation so that each process of the investigative process can be carried out effectively. DFIs might require different sets of tools and techniques to be able to carry out each given process in the investigative process. Therefore, this aspect of the digital investigative process has been incorporated into the CDFIPM as an Overriding Principle, namely Prepare and Test Tools and Techniques, that will need to be followed throughout all the other Processes of the model. This Principle has been extensively covered in technical standard documents such as ISO/IEC 27001 (2013) and ISO/IEC 17799 (2005), guidelines such as National Institute of Standards and Technology (NIST, 2015; Kent et al., 2006), as well as technical reports such as Information Assurance Advisory Council (IAAC) (Sommer, 2008).

For instance, under a comprehensive project, entitled CFTT (Computer Forensics Tools Testing), carried out by the National Institute of Standards and Technology (NIST, 2015), various methodologies have been established for testing computer forensic software tools through the development of general tool specifications, test procedures, test criteria, test sets, and test hardware. This detailed guideline provides necessary information for digital forensic tools developers to improve their tools, and also enable DFIs to make informed choices about obtaining and testing digital forensic tools and understand the tools' capabilities.

Therefore, due to the fact that tools and techniques testing and preparation have already been covered in detail, this thesis does not aim to focus on this aspect of the investigative process in more details. However, some examples on certain steps that DFIs will need to undertake in relation to this Overriding Principle will still be provided only for illustrative purposes. Some activities that DFIs will need to perform in relation to Prepare and Test Tools and Techniques Principle include, but are not limited to:

- determining which tools must be used for each given Process of the CDFIPM;
- identifying which tools must be utilised for different data analysis tasks;
- investigating and establishing which tools have been scientifically tested; and
- identifying the degree of error in connection with tools.

Cases where untested tools have been used to carry out digital investigations are easily challenged in courts. Therefore, one key element that DFIs will need to consider at all times under this Principle is the need to select tools that are court-proven such as EnCase, AccessData FTK, ProDiscover, Sleuthkit and Autopsy. Another important aspect that investigators will need to adhere to under this Overriding Principle is the need to have up-to-date training on how to use the latest versions of different forensic tools in order to make effective use of them.

Finally, as already stated, each Process within an investigative process might require different sets of tools. For example, to conduct the Examination Process, the software tools such as FTK and EnCase, that are capable of revealing hidden, deleted, swapped and corrupted files or performing data carving, will need to be utilised (see Appendix A for a practical illustration). In terms of techniques, for example in cases where public and private IP addresses need to be acquired and mapped to the country and institutions, IP addresses can be readily acquired by performing the following commands: ping, nslookup, dig, tracert from a DNS server. Moreover, DFIs can easily locate a county by various online tools such as IP Location (2016) or WhatIsMyIPAddress (2016) (see also Appendix A for a practical illustration).

3.10.6 Obtain and Adhere to Authorisation

Any digital investigation that is commissioned to be carried out necessitates proper authorisation, whether it is an internal or an external authorisation. In fact, each single stage of digital investigation should be authorised, and therefore an authorisation is required for each given process. Due to its significance on the investigative process, authorisation has been incorporated into the CDFIPM as an Overriding Principle, namely Obtain and Adhere to Authorisation. This Overriding Principle requires investigating organisations to obtain proper authorisation from one of the following groups: government authorities, system owners, system custodians, principles or users etc., when undertaking a digital investigation. The significance of this Principle for activities carried out during the digital investigation processes is justified by the fact that the rights of the system owners, custodians, principles or users should not be infringed. Moreover, this principle ensures that no law is violated. The environment in which digital investigation is carried out determines the type of authorisation required.

The authorisation might be needed both within a legal environment or an organisational environment. Authorisation for investigations involving law enforcement often requires a search warrant or other legal approval that requires sufficient evidence or suspicion (see section 2.3.2). For corporate incidents, search warrants are not usually required so long as the proper privacy policies are in place. This Overriding Principle must be adhered to concurrently throughout all the other Processes of the CDFIPM.

3.10.7 Maintain a Detailed Documentation

It is extremely important to document all the activities carried out throughout the entire investigative process in order to enable other investigators to authenticate the process and results. As well as being incorporated as a single Phase, documentation has also been incorporated into the CDFIPM as an Overriding Principle, namely Maintain a Detailed Documentation, that will need to be applied throughout the whole investigative process. The aim of this Overriding Principle is to record all information applicable or produced during the investigative process to support decision making and the legal, administrative processing of those decisions. This Overriding Principle involves documenting both physical and digital crime scene. For instance, documentation of the physical crime scene involves creating sketches and making video of a physical crime scene, while documentation of digital crime scene involves investigators properly documenting each item of digital evidence when it is discovered. See section 3.7.1.6 for more details on documentation.

3.10.8 Interact with Physical Investigation

A digital investigation and a physical investigation are often interrelated and dependent on one another (Carrier and Spafford, 2003). In cases where a physical investigation requires an assistance from a digital investigation, an example can be to use a digital forensic investigation to reveal communications between terror suspects via computers, mobile phones, online social network activities, email communication, communication via chat rooms and forums, etc. (Montasari, 2016, c; Valjarevic and Venter, 2015). An example of digital investigation being dependent on a physical investigation is when a suspect is interviewed to provide a password to a system under investigation (Valjarevic and Venter, 2015). In the CDFIPM, Interact with Physical Investigation has been

included as an Overriding Principle since defining the relationship between a digital investigation and a physical investigation is required to preserve chain of custody, preserve the integrity of the digital evidence, protect the digital evidence from damage and ensure an efficient investigation.

3.11 Summary of the Chapter

This chapter covered the Design and Development phase of the thesis and proposed a Comprehensive Digital Forensic Investigation Process Model (the CDFIPM), covering the entire digital investigative process. The CDFIPM is the most comprehensive, detailed and structured DFIPM presented to date. Each Process of the model was discussed and justified in this chapter. Due to its top-down approach, an overview of the model was firstly formulated specifying the first-level components, i.e. Classes. Each first-level component was further broken down to specify the second-level components, i.e. Processes. In turn, each second-level component was further refined in greater details to specify the third-level and forth-level components, namely Phases and Sub-Phases respectively. The CDFIPM is also both generic and formal, enabling DFIs to reach conclusions that are reliable, repeatable and well-documented. Due to its scientific approach, the CDFIPM will enable DFIs to follow a uniform approach, to overcome biased and predetermined theories, and authenticate their discoveries by attempting to prove themselves wrong. This, in turn, will result in well-established conclusions that support expert testimony in courts of law.

Chapter 4: Demonstration

4.1 Introduction

This chapter follows the Demonstration activity of the Peffers et al's (2006) DSRP, used in this research, and discusses the methods employed to demonstrate the potential deployment of the CDFIPM. The Demonstration activity of the DSRP requires a researcher to apply the artefact in an appropriate environment such as "experimentation" and "case study" to solve the stated problem (Hevner et al., 2010; Peffers et al., 2006). Resources needed for the Demonstration activity include effective knowledge of how the artefact should be applied to solve the stated problem. In order to assess how the CDFIPM addresses the stated research problem, two approaches have been adopted. The first approach, discussed in the **Appendix A**, involves conducting a hypothetical digital forensic investigation in a digital forensic laboratory (DFL), and the second approach, discussed in this chapter, involves applying the CDFIPM to three case scenarios and performing a walkthrough of the model. The two approaches followed are identified as being appropriate for evaluating "simulations" and "model" (Hevner et al., 2010; Adams, 2012; Peffers et al, 2006; Balci, 2004). The Demonstration activity was carried out prior to the model being submitted to the experts for independent evaluation (discussed in Chapter 5).

4.2 Case Scenario Implementation of the CDFIPM

For this part of the Demonstration activity, the 'case scenario approach', three case scenarios are followed in order to conduct a walkthrough of the entire processes of the CDFIPM to assess the model's efficacy in solving computer crimes. Each of the case scenarios demonstrates how the CDFIPM could be associated with specific aspects of an investigation being conducted in the three fields of law enforcement, commerce and incident response. All the three case scenarios are based on actual situations and are intended to demonstrate the potential deployment of the CDFIPM. Case scenario one involves a DFI working for a third-party digital forensic service provider and is derived and modelled after Adams (2012). Case scenario two pertains to the possession of contraband material (child pornography) and is modelled after Beebe and Clark's

(2005) and Carrier and Spafford's (2003) law enforcement contraband scenarios. Case scenario three relates to the exploitation of a vulnerability found in an online service operated by a bank and is modelled after Ciardhuáin (2004).

4.2.1 Case Scenario One

ValidPath is a small size company which provides financial services to its customers. The company does not have an in-house incident response team, nor does it have procedures for forensic readiness and incident detection implemented. There are only one IT manager and an additional IT staff member to maintain ValidPath's network and IT systems. ValidPath suspects one of its ex-employees, Mr. Davis, of stealing the company's confidential data such as price lists and customers' information prior to his departure to set up his own company in direct competition. ValidPath contacts their solicitor, Mr. Duncan, to raise the issue; in order to investigate the matter, Mr. Duncan contacts a third-party digital forensic service provider, RMDFSP, to investigate the issue.

Since this digital investigation does not appear to be large in scope as there is only one PC involved, the head of the digital forensic investigation team at RMDFSP, investigator R, assigns only one more person, investigator P, to this investigation. Moreover, due to the fact that ValidPath does not have an in-house incident response team and has not implemented forensic readiness and incident detection procedures in advance, this investigation will start from the Planning Process of the CDFIPM, where the investigative team from the third-party will carry out the planning and preparation for this investigation. Throughout the following stages of the digital investigative process, investigator R and investigator P adhere to all the eight Overriding Principles of the CDFIPM (see section 3.10).

Planning Process

- Investigator R holds a meeting with Mr. Duncan and the directing manager of the ValidPath Company to understand what is required. During the meeting, it becomes clear that investigator R is required to examine and analyse a desktop computer running Microsoft Windows 7 Operating System which was last used

by Mr. Davis and also ValidPath's network data related to Mr. Davis. Investigator R is required to find out whether there exists any evidence showing that Mr. Davis has accessed and removed any of ValidPath's confidential data prior to his departure. Investigator R also discusses the legal implication of this investigation with Mr. Duncan, the legal representative of ValidPath.

- Investigator R determines the number and the location of the system required to be analysed prior to attending the offices of ValidPath. It becomes apparent that there is only one PC involved running Window 7 Operating System, and the PC is located in one of ValidPath's offices.

- There is no restriction in terms of timing.

- Type of investigation is classified as an internal investigation at this point, and thus investigator R will require a written authorisation from both ValidPath as well as RMDFSP to start the investigation. Investigator R also determines that there is no external authorisation needed for this investigation.

- Investigator R performs a risk assessment to identify any safety issues concerning the safety of personnel and equipment.

- As part of planning logistics, investigator R has already selected one more person, investigator P, to assist him in conducting this investigation. He also plans the equipment, storage and the transportation of the device.

- Having conducted the previous activities, investigator R is now able to create an outline plan to carry out this digital investigation.

- Investigator R confirms that all aspects of the CDFIPM's Planning Process have been completed and therefore signs and dates a copy of the UML Activity Diagram for this Process as a file note.

Preparation Process

- Referring to the CDFIPM's Preparation Process, investigator R now implements the investigation plans that he drew from the previous Process.

- Investigator R obtains an internal written authorisation from both his company as well as the ValidPath to carry out the investigation.

- Based upon RMDFSP's procedures, investigator R prepares appropriate imaging tools as well as two blank external hard drives which have already been verified for integrity.

- Investigator R tasks investigator P to conduct the data acquisition.

- RMDFSP issues the ValidPath a letter of engagement setting out the terms and conditions under which the investigation will be conducted in addition to describing the scope of the work required.

- Investigator R confirms that all aspects of the CDFIPM's Preparation Process have been completed and therefore signs and dates a copy of the UML Activity Diagram for this Process as a file note.

Secure and Evaluate Crime Scene Process

- Investigator R and investigator P attend the offices of ValidPath with the equipment that they have already prepared as part of the logistical preparation from the previous Process.

- The first step that they take into account is to address safety issues to ensure that there is no danger to their own safety as well as the safety of the ValidPath Company's employees and the equipment.

- Throughout the entire process, a detailed documentation of all activities is maintained.

- As part of carrying out an onsite preliminary survey, investigator R consults with the ValidPath's IT manager, who is involved in the day-to-day operation of the company's IT systems, in order to obtain information concerning the location of the desktop computer under investigation and the potential digital evidence.

- The IT manager directs investigator R and investigator P to the location of the desktop computer. In order to preserve data held on the desktop computer, investigator R isolates the PC with the co-operation of investigator P and the IT manager.

- Now that the preliminary survey has been carried out and all the necessary information has been obtained, investigator R is able to update the outline plan to create a plan for data acquisition onsite.

- The plan for onsite data acquisition includes the onsite acquisition of data on Mr. Davis' desktop computer which is running at this point and also the live acquisition of Mr. Davis' profile data stored on ValidPath's fileserver.

- Investigator R confirms that all aspects of the Secure and Evaluate Crime Scene Process of the CDFIPM have been completed. A copy of the UML Activity Diagram for this Process is signed and dated by investigator R as a file note to show that this Process is now complete.

Identification Process

- Investigator R instructs investigator P to acquire data from the hard drive of Mr. Davis' desktop computer.

- Investigator P surveys and searches the digital crime scene to identify any data representing potential digital evidence.

- Since it is not a law enforcement investigation and there is no timing constraint imposed to acquire data, investigator R instructs investigator P not to carry out an onsite triage.

- Investigator R signs and dates a copy of the Activity Diagram for the Identification Process to confirm that this Process has been completed.

Acquisition and Collection Process

- Investigator R confirms that the desktop computer used by Mr. Davis prior to his departure has not been seized by ValidPath's IT manager and is currently in operation.

- Referring to the UML Activity Diagram for the CDFIPM's Acquisition and Collection Process, investigator R considers it the most appropriate that both a live and a static data acquisition must take place onsite.

- Investigator R determines that live data acquisition from ValidPath's network should be performed to acquire the profile data concerning Mr. Davis' activities.

- Investigator R attaches a forensically clean external hard drive (the master hard drive) which has already been verified for integrity and labelled based on the RMDFSP's procedures to a computer connected to ValidPath's network.

- Using the FTK Imager, based on the RMDFSP's procedures for acquiring live network data, investigator R captures the profile data related to Mr. Davis from the ValidPath's fileserver. This forensic image is created on the master hard drive.

- Investigator R duplicates the acquired master image and creates a back-up image (working copy) which is placed on a different blank hard drive (back-up hard drive) that has already been checked for integrity and labelled based upon the RMDFSP's procedures.

- Hash verification values for both the master copy and the working copy of the network data image are then calculated and recorded on the Evidence Acquisition form produced by RMDFSP.

- At this point, investigator R confirms that the live data acquisition from the ValidPath's network has been completed.

- In addition to performing live acquisition of the network data, investigator R also considers it most appropriate that an onsite static data acquisition must be performed from the hard drive of the desktop computer last used by Mr. Davis prior to his departure.

- Investigator R instructs investigator P to perform an onsite data acquisition from the hard drive of the desktop computer after it has been shut down.

- Investigator P checks and confirms that the desktop computer is running. He photographs the PC including its screen and records its details such as serial and model number, etc. on an Evidence Acquisition form produced by RMDFSP.

- Based on the RMDFSP's SOPs, investigator P confirms that data held on the computer is stable; therefore, he removes the power source directly from the back of the desktop computer and shuts down the PC.

- According to the CDFIPM's requirement for forensically sound data acquisition and based upon the RMDFSP's SOPs, prior to the data acquisition, investigator R utilises a physical write-blocking tool to avoid altering the original data contained in the desktop's hard drive.

- Referring to the steps shown in the Acquisition and Collection Process of the CDFIPM for acquiring a forensic image of a hard drive, investigator P images the hard drive of the desktop using a court approved forensic tool (such as AccessData FTK Imager or EnCase) based on the RMDFSP's SOPs.

- Using an appropriate imaging tool, investigator P creates a raw image of the desktop's hard drive (the master image) on a forensically clean hard disk (the master disk) that has been checked in advance for integrity and labelled based on the RMDFSP's digital forensic procedures.

- Investigator P also duplicates the acquired image of the desktop computer's hard drive (the master image) and creates a working copy on which the subsequent examination and analysis will be performed. The working copy of the master image is created on a separate blank hard drive which has also been verified in advance for integrity.

- Hash verification values for both the master copy and the working copy of the hard drive image are then calculated and recorded on the Evidence Acquisition form produced by RMDFSP.

- Investigator P reports back to investigator R that the static data acquisition from the hard drive of the desktop computer previously used by Mr. Davis has now been completed.

- Investigator P reassembles the desktop computer and returns it to the IT manager who checks that the PC is operational and connects it to ValidPath's network.

- Investigator R instructs investigator P to label and package the external hard drives containing the forensic images of both the network data as well as the desktop's hard drive data for transportation.

- Investigator P packages and labels the two hard drives and confirms that the documentation associated with the two hard drives are accurate. Based on the CDFIPM's Overriding Principles, investigator P also completes a Chain of Custody form produced by RMDFSP for the two external hard drives.

- The two hard drives are transported and stored in a secure storage facility at the RMDFSP for later examination and analysis.

- Investigator R confirms that the Acquisition and Collection Process of the CDFIPM is now complete by signing and dating a copy of the Activity Diagram for this Process as a file note.

Examination Process

- Back at RMDFSP, investigator R tasks one of his digital forensic analysts (DFA), investigator B, with examining and analysing the acquired data to determine whether there is any evidence linking Mr. Davis to the removal of the confidential data from ValidPath.

- Investigator R provides investigator B with a Job Request Document form produced by RMDFSP outlining the description of work to be carried out. Furthermore, based on the RMDFSP's SOPs, investigator B is provided with an Evidence Sought form outlining the types of evidence needed to link Mr. Davis with stealing ValidPath's confidential data.

- Investigator B takes the custody of the back-up hard drive containing the working copies of the acquired data from the storage facility and signs and dates a Chain of Custody form produced by RMDFSP indicating that he has taken the custody of the device.

- Prior to starting the examination of the acquired hard drive and network data, investigator B prepares a plan of action based upon the steps outlined in the Examination Process of the CDFIPM. As part of the preparation, investigator B prepares a forensic workstation with sanitized storage space and installs legally approved forensic tools on the workstation. Other preparation activities that investigator B performs include: keeping an audit trail of all of the steps undertaken during this process in the form of note taking, developing an initial hypothesis and prediction based on the information received by investigator B, and experimentation and testing.

- Once the preparation has been completed, investigator B initiates the Examination Process by importing each set of digital evidence to the forensic examination software installed on the forensic workstation separately. Referring to the Examination Process of the CDFIPM, investigator B applies each step of the Examination Process to each data set to develop a more comprehensive and methodical approach to this forensic investigation.

- Investigator B extracts each data set (makes the potential digital evidence visible) into a readable form by mounting it on the forensic software which he has previously installed on the forensic workstation. Using the automated function of the forensic software, investigator B indexes files and folders to give structure to each acquired data set and retrieves obfuscated data such as partially deleted files from the original desktop computer used by Mr. Davis.

- Referring to the Examination Process of the CDFIPM, investigator B surveys each acquired data set in order to develop an overall familiarity with the totality of evidence to find items of potential relevance to the investigation. While examining data acquired from both the hard drive of the desktop used by Mr. Davis and ValidPath's network, investigator B identifies several confidential documents related to ValidPath's price lists and customers' data. Also, examining ValidPath network's log files, investigator B is able to link the downloads of the company's confidential files to the IP address of the desktop computer that Mr. Davis had logged onto.

- Referring to other Phases within the Examination Process of the CDFIPM, investigator B performs data harvesting, organisation, reduction and classification in order to produce a reduced and organized dataset which will be fed into the Analysis Process at a later stage in the investigation to expedite the Analysis Process.

- Investigator B records items of evidence found during this Process on an Evidence Record form produced by RMDFSP.

- Investigator B confirms that all activities related to the Examination Process of the CDFIPM is now complete by signing and dating a copy of the Activity Diagram for this Process as a file note.

Analysis Process

- Investigator R joins investigator B to perform the Analysis Process of the CDFIPM.

- Referring to the Analysis Process of the CDFIPM, the investigative team are now able to formulate a detailed hypothesis which is based on the facts deduced from the Examination Process.

- The investigative team test the data which they reduced and organised in the previous Process against the hypothesis to determine the legal validity of the digital evidence. The investigative team is able to attribute the theft of ValidPath's confidential data to Mr. Davis.

- The investigative team also determine that their formulated hypothesis proving that Mr. Davis has indeed stolen ValidPath's confidential data holds true.

- At this stage, investigator R confirms that the Analysis Process of the CDFIPM is complete and signs and dates a copy of the Activity Diagram for this Process as a file note.

Interpretation Process

- Now that the investigative team have been able to evaluate their findings, and their hypothesis holds true, by referring to the Interpretation Process of the CDFIPM, the investigative team interpret the evidence and produce meaningful statements for use in legal proceedings.

- The investigative team describe the facts that they have found during the Analysis Process and compare and prioritize digital evidence artefacts they have gathered.

- Investigator R confirms that the Interpretation Process of the CDFIPM is complete by dating and signing a copy of the Activity Diagram for this Process as a file note.

Event Reconstruction Process

- Referring to the Event Reconstruction Process of the CDFIPM, the investigative team consolidate and review their findings. Their assessment of their developed hypothesis shows that they have acquired all the necessary evidence which shows that Mr. Davis has indeed stolen the ValidPath's confidential data.

- The investigative team use the sequence of events that they have deduced from the digital evidence, and reconstruct a sequence which shows the investigation results accurately.

- The investigative team are able to explain how Mr. Davis was able to remove confidential data from ValidPath's network.

- Investigator R confirms that the Event Reconstruction Process of the CDFIPM is complete and signs and dates a copy of the Activity Diagram for this Process.

Reporting Process

- Investigator R tasks investigator B to produce a forensic report detailing not only the outcome of the Analysis Process but also the entire investigation. A copy of this report is also kept with the RMDFSP as a classified document.

- Investigator B confirms that the Reporting Process of the CDFIPM is complete and signs and dates a copy of the Activity Diagram for this Process.

Presentation Process

- Investigator R meets initially with the RMDFSP's management and presents the findings of this investigation. He then holds a meeting with ValidPath and their legal representative, Mr. Duncan, and presents the investigation findings.

- During the meeting, various issues such as financial damage to ValidPath and legal implications concerning the investigation are discussed.

- Investigator R confirms that the Presentation Process of the CDFIPM is complete and signs and dates a copy of the Activity Diagram for this Process.

Investigation Closure Process

- Investigative R reviews the outcome of the investigation and confirms that all of the necessary evidence has been acquired.

- ValidPath accepts the hypothesis that investigator R has presented to them as the acquired digital evidence against Mr. Davis is strong in terms of relevance, admissibility and weight.

- Based upon the findings presented by RMDFSP, ValidPath's management decide to report the incident to the police and seek to bring charges against Mr. Davis. RMDFSP confirms to ValidPath, through investigator R, their desire to give evidence in a court if the need arises.

- ValidPath identifies the lessons learnt and realise that they should implement forensic readiness procedures as well as mechanisms for an early incident detection.

- Back at RMDFSP, investigator R communicates the results of findings also to the RMDFSP's management and records the findings of this investigation on a database for the future reference.

- As far as RMDFSP is concerned, this digital investigation is complete from their end as the law enforcement will be involved from this point forward.

- Investigator R confirms that the Investigation Closure of the CDFIPM is now complete and signs and dates a copy of the Activity Diagram for this Process as a file note.

Future Readiness Process

- ValidPath starts applying the lessons that they have learnt from this incident by seeking to implement appropriate forensic readiness procedures and incident detection systems.

- Investigator R provides ValidPath with a set of recommendations on how they can improve in terms of securing their digital data assets.

- Investigator R tasks his investigative team to develop a case study based on this investigation for future training of other investigators.

- Investigator R confirms that the Future Readiness Process of the CDFIPM is complete and signs and dates a copy of the Activity Diagram for this Process as a file note.

- RMDFSP, through investigator R, offers to provide further services to ValidPath, expressing their desire to give expert witness in a court in case Mr. Davis appears before a judge due to his theft of company's confidential data.

4.2.2 Case Scenario Two

Based on gathered intelligence and a search warrant acquired, police raids the residence of Mr. Thomson, who is suspected of having downloaded and distributed indecent images of minors. During the police raid, a single desktop computer which is powered off, and that is thought to contain potential evidence is found. Upon questioning Mr.

Thompson, it is confirmed that the desktop computer belongs to him. Police seizes the desktop computer and arrests Mr. Thompson. The Case Officer, the head of the High-Tech Crime Unit (HTCU), Officer Lloyd, who is in charge of the digital investigation, is requested to analyse the content of the seized desktop computer.

Readiness Process

- The HTCU has already developed both operational and infrastructure readiness capabilities and has its own Standard Operating Procedures (SOPs).

- The Case Officer, Officer Lloyd, dates and signs a physical copy of the UML Activity Diagram for the CDFIPM's Readiness Process to confirm that this process has already been implemented prior to this incident.

Incident Detection Process

- Mr. Thompson's wife discovers that he has downloaded and stored incident images of minors on his computer, and as a result she reports him to the police.

- Police confirm the initial reporting of the crime[30] and prepares for further action.

- Referring to the Incident Detection Process of the CDFIPM, police classify the incident as severe, and the incident is described as the possession and distribution of indecent images of minors.

- The Case Officer, Officer Lloyd, confirms that the Incident Detection Process of the CDFIPM is complete by dating and signing a copy of the Activity Diagram for this process as a file note.

[30] For instance, they might have already covertly monitored Mr. Thomson's online browsing activities and chat logs based on a proper authorisation that they have acquired.

First Response Process

- Referring to the First Response Process of the CDFIPM, the Case Officer, Officer Lloyd, confirms that this Process is not applicable[31] to the law enforcement by dating and signing a copy of the Activity Diagram for this Process as a file note.

Planning Process

- Officer Lloyd, confirms that his unit is required to examine and analyse the content of the desktop computer belonging to Mr. Thompson which is suspected of storing indecent images of children. Officer Lloyd and his investigative team are expected to find out whether there exists any evidence proving that Mr. Thompson has downloaded and distributed indecent images of minors.

- Based on the CDFIPM's Planning Process, the type of investigation is classified as criminal; thus, it is determined that a search warrant is required to allow the police to search Mr. Thompson's property and to seize his desktop computer.

- Officer Lloyd considers the physical, timing and data constraint. It is determined that there is only one single property to search and only one single desktop computer involved. The type of data that the police is interested in is also determined. This includes, but is not limited to, JPG, PNG and GIF or other image file formats, as well as logs containing records of Mr. Thompson's online chat sessions.

- Officer Lloyd also performs a risk assessment concerning the personnel and the equipment safety. As part of this assessment, Officer Lloyd discovers that Mr. Thompson has had the history of violence in the past. He, therefore, requests additional back up officers.

[31] In the context of law enforcement investigations, the CDFIPM's "Secure and Evaluate Crime Scene Process" covers activities associated with the first response.

- Officer Lloyd also plans the logistics for the transportation and storage of the evidence. Officer Lloyd selects two additional personnel from the HTCU to be involved in the investigation and assigns them different roles based on their training and skills. Officer Wilson is to conduct the data acquisition, and Officer Morris is to perform the subsequent data analysis.

- Referring to the CDFIPM's Planning Process, Officer Lloyd creates an outline plan for this digital investigation based on all the planning activities that he has carried out.

- Officer Lloyd confirms that this process is complete by dating and signing a copy of the UML Activity Diagram for the CDFIPM's Planning Process as a file note.

Preparation Process

- Referring to the CDFIPM's Preparation Process and based on the HTCU's Standard Operating Procedures (SOPs), Officer Lloyd implements the planning activities that he has drawn in the Planning stage of the CDFIPM.

- The search warrant is acquired and the equipment prepared according to the HTCU's SOPs.

- Referring to the CDFIPM's Preparation Process and based on the HTCU's SOPs, Officer Wilson and Officer Morris prepare and validate forensically sound techniques based on the roles which they have been assigned.

- To confirm that the Preparation Process of the CDFIPM is complete, Officer Lloyd dates and signs a copy of the UML Activity Diagram for this Process as a file note.

Secure and Evaluate Crime Scene Process

- Police raids Mr. Thompson' residence. Along with the other police officers[32], Officer Lloyd and Officer Wilson also attend the crime scene. Officer Wilson has been assigned with the task of data acquisition.

- Referring to the CDFIPM's Secure and Evaluate Crime Scene Process and based on the HTCU's SOPs, Officer Lloyd addresses the safety issues in collaboration with other officers.

- Officer Lloyd instructs other police officers not to tamper with any digital device they encounter in order to preserve the crime scene.

- Mr. Thompson is detained and questioned briefly about the location of his desktop computer or any additional digital device he might possess. It is confirmed that he possesses only one single desktop computer.

- Officer Lloyd carries out a preliminary survey which includes the consideration for a mixture of both onsite and offsite data acquisition and identification of any technical issues.

- Officer Lloyd updates the initial Outline Plan he created in the Planning Process, now that he has attended the site of crime scene and has a better picture of the incident.

- Officer Lloyd dates and signs a copy of the UML Activity Diagram for the Secure and Evaluate Crime Scene Process to confirm that this Process is complete.

[32] This refers to the primary officers and not the digital forensic investigators.

Identification Process

- Referring to the activities included in CDFIPM's Identification Process, officers locate Mr. Thompson's desktop computer, suspected of containing indecent images of minors.

- Since the collected intelligence does not suggest any child abduction or exploitation, missing person or a life-threatening circumstance, Officer Lloyd determines that there is no need to perform an onsite examination of the desktop computer.

- Officer Wilson assigned with the data acquisition task determines that the desktop computer is already powered off. Since the warrant permits the seizure of the computer, it is decided to carry out the data acquisition back at the forensic laboratory.

- To confirm that the Identification Process of the CDFIPM is complete, Officer Lloyd dates and signs a copy of the UML Activity Diagram for this Process as a file note.

Acquisition and Collection Process

- Referring to the Acquisition and Collection Process of the CDFIPM, Officer Wilson confirms that the desktop computer that is to be seized is in off state. He photographs the desktop computer and notes down its serial and model number.

- In accordance with the Acquisition and Collection Process of the CDFIPM, Officer Wilson records, removes and secures the desktop connection based on their own SPOs. He proceeds with labelling and packaging the desktop computer including its accessories.

- The desktop computer is transported back to the police department where it is stored in a safe storage facility.

- Officer Lloyd instructs Officer Wilson to obtain the desktop computer from the storage and perform the data acquisition. Officer Wilson takes the custody of the desktop computer and signs a Chain of Custody form, checks the documentation and condition of the device and confirms that he has not detected any sign of damage.

- Referring to the CDFIPM's Acquisition and Collection Process, based on the HTCU's SOPs, Officer Wilson decides on the most appropriate means of acquiring data and performs a data acquisition on the desktop's hard drive.

- The acquired image is created on a forensically clean external hard drive that has already been verified for integrity. Officer Wilson also duplicates the acquired image on a different forensically clean external hard drive to become the working copy.

- Referring to the Acquisition and Collection Process of the CDFIPM, Officer Wilson verifies the two sets of acquired images and confirms that neither the original evidence nor the working copy has been modified. The calculated hash verification values are recorded for both the master copy and the working copy on the Evidence Acquisition form produced by the HTCU.

- Officer Lloyd confirms that the CDFIPM's Acquisition and Collection Process in now complete by dating and signing a copy of the UML Activity Diagram for this Process as a file note.

Examination Process

- Officer Lloyd tasks Officer Morris, who has an extensive expertise in the digital evidence analysis, to conduct the examination and analysis of the acquired data.

- Officer Morris takes the custody of the hard drives containing the master image and working image of the original evidence. He checks the state of the devices and confirms that he has not detected any damage to the hard drives by dating and signing a Chain of Custody form produced by the HTCU.

- Based on the HTCU's SOPs, Officer Morris prepares a forensically clean workstation with appropriate software installed on it into which the acquired working copy will be imported for the forensic examination and analysis of the acquired data.

- Prior to carrying out the Examination Process, Officer Morris checks the Acquisition and Collection form filled in by Officer Wilson and confirms that the acquired data has already been verified for integrity.

- Referring to the Examination Process of the CDFIPM, Officer Morris carries out the digital evidence examination using appropriate and court approved forensic tools based on the HTCU's SOPs.

- Officer Morris is able to recover many artefacts showing that Mr. Thomson possessed and distributed pornographic images of children. Various documents with JPG, GIF and PNG file formats depicting indecent images of minors are discovered from various locations on the computer's hard drive. Officer Morris also finds certain chat logs showing Mr. Thompson's conversation with other individuals with the same motives.

- Referring to the activities contained in the Examination Process of the CDFIPM, due to a large amount of data to be examined, Officer Morris reduces, harvests and organises the data in order to expedite the investigation in the Analysis Process, where he will look into the discovered evidence in more details.

- Officer Morris records the details of the evidence he has found on the Evidence Found form produced by the HTCU.

- He then confirms that the Examination Process of the CDFIPM is now complete by dating and signing a copy of the Activity Diagram for this Process as a file note.

Analysis Process

- Referring to the Analysis Process of the CDFIPM, Officer Morris now performs further analysis on digital evidence that he has recovered from the working image.

- He formulates a hypothesis based on the investigation findings in which he is able to attribute the downloaded indecent images stored on the desktop computer's hard drive to Mr. Thomson.

- To confirm that the Analysis Process of the CDFIPM is now complete, he dates and signs a copy of the Activity Diagram for this Process as a file note.

Interpretation Process

- Based upon the Interpretation Process of the CDFIPM, Officer Morris interprets digital evidence resulting from the Examination Process and the Analysis Process and produces meaningful statements in the legal context.

- He then describes the facts that he has found during the Analysis Process and compares and prioritizes digital evidence artefacts he has gathered.

- Officer Morris confirms that the Interpretation Process of the CDFIPM is now complete by dating and signing a copy of the Activity Diagram for this Process as a file note.

Event Reconstruction Process

- Now that Officer Morris has completed the Interpretation Process of the CDFIPM, he is able to reconstruct a possible event sequence which reflects the incident result accurately. To do so, he uses a series of events that he has deduced from digital evidence.

- To ensure that he has acquired all the evidence required to support his formulated hypothesis, Officer Morris asks one of his colleagues in the HTCU with the same expertise, investigator Anderson, to test the review results independently against the original hypothesis. Investigator Anderson tests the review results against the original hypothesis and confirms that all the evidence has been acquired.

- Officer Morris confirms that the Event Reconstruction Process of the CDFIPM is now complete, and he dates and signs a copy of the Activity Diagram for this Process as file note.

Reporting Process

- Referring to the CDFIPM's Reporting Process, Officer Morris writes a detailed report detailing the outcome of his analysis and the investigation as a whole.

- He then confirms that the CDFIPM's Reporting Process is complete by dating and signing a UML Activity Diagram for this Process as a file note.

Presentation Process

- Referring to the Presentation Process of the CDFIPM, the Case Officer, Officer Lloyd, holds a meeting with both Officer Wilson and Officer Morris instructing them that they are required to prepare an expert testimony based on the report produced.

- Officer Lloyd confirms the main target audience as judge, jury, the prosecutor, the accused, Mr. Thompson and his legal representative, as well as other police personnel. Also, during the meeting, Officer Lloyd and the two other officers discuss the appeal process and the legal implications of this phase of the investigation during the meeting.

- Officer Wilson and Officer Morris prepare the expert testimony which will be delivered to the court along with the produced report and all the relevant evidence collected and analysed during this investigation.

- In the court, the digital evidence is challenged by the defence. However, since the Officers adopted scientific methods employing the CDFIPM to conduct the digital investigative process, the jury finds Mr. Thompson guilty.

- Officer Lloyd now confirms that the CDFIPM's Presentation Process is complete by signing a copy of the Activity Diagram for this Process as a file note.

Investigation Closure Process

- Officer Lloyd and his investigative team hold a meeting and review the entire investigation and discuss any lessons they have learnt from this particular investigation. Areas of improvement for future investigations are discussed and addressed.

- It has also been decided that Mr. Thompson's desktop computer is stored for a period of time before it will be destroyed.

- Officer Lloyd holds a meeting with his senior manager to communicate the results of the investigation.

- He also tasks Officer Morris to record the case decision on a database as a record for the future reference.

- To confirm that the Investigation Closure Process of the CDFIPM is now complete, Officer Lloyd dates and signs a copy of the Activity Diagram for this Process as a file note.

Future Readiness Process

- Referring to the Future Readiness of the CDFIPM, Officer Lloyd makes a set of recommendations to his team members concerning the areas of improvements. He also tasks Officer Morris and Officer Wilson with developing a case study based on this investigation to assist the future investigations.

- Officer Lloyd dates and signs a copy of the Activity Diagram for the Future Readiness Process of the CDFIPM as a file note to confirm that this process is now complete.

- Finally, Officer Lloyd confirms that this investigation is now complete by dating and signing an Investigation Closure Document form produced by the HTCU.

4.2.3 Case Scenario Three

This investigation started when Bank X in London (England) received an email claiming to have found a vulnerability in an online service operated by the bank. The email offered to provide details of the vulnerability in exchange for payment. On checking their logs, Bank X concluded that an unauthorised access had been made to their web server. The bank received further emails threatening to reveal the vulnerability to the press and public, including a link to a website which the suspect intended to use to disclose the vulnerability. Bank X reported the issue to the police in London who initiated the investigation. It became obvious that the compromised web server was located in Manchester (England) from Bank X's headquarters and that the source of the emails was in Cardiff (Wales). Therefore, another police force, namely SWP (the South Wales Police), took up the case to start the investigation.

Readiness Process

- Bank X has already implemented both operational and infrastructure readiness capabilities, and has an in-house incident response team and procedures for forensic readiness and incident detection implemented. The bank also has its own Standard Operating Procedures (SOPs).

Incident Detection Process

- The first step in this investigation is the Incident Detection and the creation of awareness that the investigation is needed. In this case, the incident has been reported by the suspect himself to Bank X. After the incident has been detected, the bank requests its senior IT Administrator, Mr. Thompson, to look into the issue to confirm or refute the validity of the incident as this might be a hoax. Mr. Thompson contacts the head of the incident response team for assistance in this matter. To validate and assess the incident, Mr. Thompson and the incident response team examine the emails and log files and confirm that the system's security has been compromised.

  Bank X then reports the incident to the London MPS (Metropolitan Police Service), who initiates the investigation of its own. It becomes clear that the compromised web server is based in Manchester and that the suspect is located in Cardiff; therefore, the investigation is passed to SWP (the South Wales Police). Up to this point, the reporting of the incident has taken place three times: when Bank X receives the emails, when the bank reports it to the MPS, and when the investigation is passed to the second police force, SWP. During this Process, both internal and external authorisation are needed. The internal authorisation is obtained when Bank X instructs its senior IT administrator to conduct the investigation. The external authorisation is acquired when the MPS realizes that SWP are the police force who are authorised to carry out the investigation. The search warrant is the example of this authorisation. Moreover, during this process detailed and contemporaneous documentation are made.

First Response Process

- Due to the fact that this incident involves law enforcement and is investigated externally, this Process is only partly applicable to this case scenario. The application of this process is when the incident response team assists the senior IT administrator in examining the log files.

Planning Process

- The Planning activity is conducted by both Bank X and the two police forces. This activity takes place in the bank's investigation when they perform an examination of the logs and decide to involve the police based on what they have found. The Planning activity also takes place in the two police forces investigations where they plan their own respective approaches to be undertaken to identify the suspect and collect the needed evidence. Under the Planning stage, the two police forces consider data constraint, timing constraint, physical constraint, and authorisation, as well as performing risk assessment, planning logistics and creating their own outline plans.

Preparation Process

- Under the Preparation activity, Bank X and the two polices forces simply implement the plans that they have drawn in the Planning stage.

Secure and Evaluate Crime Scene Process

- This activity takes place when the SWP police officers raid the premises of the suspect's place of employment. The first step they take is to address the safety issues such as the safety of the officers and employees, followed by preserving the crime scene. Since the suspect is at the crime scene, he is detained and briefly interviewed as the authorisation allows the questioning of the suspect. Investigators then survey the crime scene in order to determine the location of digital device(s) and establish the combination of onsite and offsite data acquisition. Throughout the entire process, detailed contemporaneous notes of all activities are maintained.

Identification Process

- Identification initially takes place when Bank X identifies their log files to determine what has occurred. Both police forces, MPS and SWP, later carry out the same activity to locate the sources of the emails. Moreover, SWP conducts a physical search which results from the information obtained from the previous

searches. Secure and Evaluate Crime Scene Process and Identification Processes both overlap as each Process requires searching the physical crime scene.

Acquisition and Collection Process

- This Process takes place when the search of the employer's premises in the previous Process led to the seizure of a computer. Since the suspect's computer system is not a mission-critical system and the authorisation permits its seizure, the investigators decide to size the system and conduct an offsite data acquisition in the police forensic laboratory. However, since the system is running, officers decide to conduct a live acquisition of volatile data first prior to shutting down the system in case the RAM might contain valuable information which might be lost after powering down the system. Using FTK, the officers perform a live acquisition of the volatile data and duplicate the master copy of the captured image of RAM. Both copies are then verified using MD5 and SHA1 checksums. Since the data on the system is stable, the officers remove the power source directly from the suspect's computer. They then record, remove and secure connections prior to labelling and packaging the system.

  The Transport Phase takes place when the system is seized and physically transferred to the police. This phase also occurs in three other occasions including: when the captured image of the RAM is taken to the police, when log files are transferred from server to the police for later examination and analysis and when the emails are transferred from the bank to the police. The Storage Phase occurs when the police retain the seized computer, the captured images of both hard drive and RAM, log files as well as emails in a secure storage facility. In the forensic laboratory, the investigators image the hard drive of the system and verify it using MD5 and SHA1 checksums. They also duplicate the master copy to become the working copy on which the subsequent Examination and Analysis will be performed.

Examination Process

- This activity initially occurs when the bank examines their log files. It also occurs when the police examine log files, emails and the working copy of both hard drive and RAM images of the suspect's system in the forensic laboratory. During the Examination Process, investigators process the deleted and hidden data to ensure that emails and log files are recognised from the evidence. Investigators also harvest data to provide structure to data which they are interested in so that it can be mounted on the investigating machine. Since the suspect's system contains large amount of data such as known systems files, investigators use metadata and unique identifiers to reduce the data by removing known system files and different other application data. The investigators are now left with the log files and the emails that the suspect sent to Bank X. Now, the emails can be uniquely attributed to the suspect who has been the user of that specific system.

Analysis Process

- This Process initially takes place when Bank X's system administrator, Mr. Thompson, and the incident response team conclude from the log files that an unauthorised access has been made to their web server. Later on, this Process is conducted in a forensic laboratory by investigators who develop the initial hypothesis for the identity of the suspect and for the manner in which the incident has taken place.

Interpretation Process

- This Process occurs after investigators evaluate their findings in the Analysis Process and determine that their formulated hypothesis is true. During this Process, investigators interpret digital evidence to produce meaningful statements for later reporting and presentation regarding how the suspect made an unauthorised access to Bank X's web serve. As part of this Process, investigators classify and organize the interpreted evidence such as log files and

emails according to their relevance in order to distinguish which digital evidence items are more important than the others.

Event Reconstruction Process

- This process occurs when investigators reconstruct the events which led to the identification of the suspect and the subsequent seizure of the suspect's computer. This entails the investigators iterating in the CDFIPM, and results in a more detailed hypothesis. Through this Process, investigators are able to explain how the suspect has carried out the intrusion to Bank X's web server. Investigators consolidate and review their findings prior to assessing the results of their review against the original hypothesis that they have formulated. Through this assessment, investigators ensure that they have gathered all relevant evidence related to that attack to support their hypothesis.

Reporting Process

- This Process takes place when investigators compile a report based on their findings to be presented in a court.

Presentation Process

- This Process occurs five times during the entire investigation. This includes: when the bank's IT Administrator presents the evidence to the management within the bank, when the bank approaches the MPS Police and present their evidence to investigators, when the MPS Police pass the investigation to SWP, when evidence is presented to acquire a search warrant and when investigators present the evidence in the court. The formality of the evidence increases as the investigation proceeds. Prior to presenting the findings to the court, investigators meet with the legal team to understand the presentation requirements. Through the meeting, the target audience in the court are determined. Investigators also carry out the necessary preparation prior to attending the court such as preparing expert testimony, exhibits and appropriate presentation aids.

During the presentation in the court, investigators are able to assist the judge and jury in understanding the technical points made by avoiding complex arguments and delivering their conclusion in a logical and structured manner. The presentation contains factual data that investigators have deduced. Moreover, investigators use the CDFIPM to enable the judge to comprehend the processes that they have followed during the investigation. In the court, the investigators have to prove and to defend the validity of the hypothesis as it is challenged by the court and the defence lawyers. Since investigators have followed a formal model which enabled them to carry out the investigation in a forensically sound manner, the opposite hypothesis is refuted. The court decides that the suspect has made an unauthorised access to Bank X's web server and sentences him to prison.

Investigation Closure Process

- This Process takes place after a formal decision is reached by the court concerning the incident. During this Process, based on the outcome of the investigation, Bank X reviews its existing policies and procedures concerning its IT security. As there is no need to backtrack to the previous stages in the investigation, bank management decide to accept the hypothesis. During this Process, the bank identifies the lessons learnt and the suspect's system is returned to his employer's company. The result of the case is recorded on the database for the future readiness. The final phase of this activity is Disseminate Investigation Results, where relevant information concerning this incident and its outcome are communicated to all stakeholders. The initial communication is carried out prior to the completion of the trial in order to remove the sensitive data from the disseminated information. The final phase, the Review Phase, discusses how the incident could have been handled better. One outcome is to install the central log server sooner than planned. The Review Phase includes a review of the investigation and identifies some new analysis techniques that are employed. The techniques are added to the official analysis procedures. During the analysis, new suspect files are identified, and they are added to the hash database so that they can be quickly found in the future investigations.

Future Readiness Process

- This activity takes place both in Bank X and also the two police forces. Bank X starts applying the lessons that they have learnt from this incident; a set of recommendations are made on how they can improve in terms of securing their digital data assets. As a result, they improve their existing forensic readiness procedures and incident detection systems. The two police forces also develop case studies based on this particular investigation for future training of other officers.

4.3 Summary of the Chapter

This Chapter followed the Demonstration activity of the Peffers et al's (2006) DSRP and discussed the methods employed to demonstrate the potential deployment of the CDFIPM. In order to assess how the CDFIPM addressed the stated research problem, two approaches were adopted. The first approach discussed in the **Appendix A** involved conducting a hypothetical digital investigation in a DFL. This approach successfully demonstrated essential investigative techniques associated with the 'Investigative Processes Class' of the CDFIPM, that could be used to answer the investigative questions of who, when, where and how. The second approach discussed in this chapter involved applying the CDFIPM to three case scenarios and performing a 'walkthrough' of the model. The walkthrough of the CDFIPM employing the three case scenarios successfully mapped the entire Processes of the model to the corresponding activities carried out by DFIs operating in the three fields of law enforcement, commerce and incident response. Having completed the Demonstration activity, the next stage in the Peffers et al's (2006) DSRP is the Evaluation activity, which is conducted by a number of DFIs, legal practitioners, experts and researchers in the field of digital forensics and is discussed in the following chapter.

Chapter 5: Evaluation

5.1 Introduction

A model has 'utility' if it is practical, applicable and appropriate; this denotes that there must be an advantage to using the model. The model has 'usability' if it is easy to be employed in order to achieve its stated goal. An effective model should, therefore, have both utility and usability. If the model does not meet the two components of usability and utility, the question will then arise as to why it was developed in the first place. If the artefact is so difficult to use that its users are discouraged from employing it, then its value is greatly reduced and its advantages are lost. Thus, the artefact needs to be evaluated in order to determine whether it has achieved both utility and usability. To evaluate a process model, five questions will ultimately need to be answered (Wise et al., 2013; Groesser and Schwaninger, 2012; Cook and Skinner, 2005; Barlas, 1996):

1. Is the model theoretically valid (Adams, 2012)?
2. Is the model usable (Adams, 2012)?
3. Does the model provide explanatory or guiding power for the user (Adams, 2012)?
4. Has the model been built right? and
5. Has the right model been built?

In relation to question 1 above, the validity of a process model derives from the extent to which it conforms to guiding principles, based on which the process is structured (Adams, 2012). Concerning question 2, the model has usability if its intended user community are able to apply it in real life situations to organise their activities to proceed through the process and produce the required results efficiently (Adams, 2012). In terms of question 3, the model has guiding power if it directs the process, suggests some sequences of activity and warns against the others (Adams, 2012). Regarding question 4, the model has been built right if it meets all the stated requirements levied upon it, and is internally complete, consistent, and accurate enough to fulfill its stated aim. Concerning question 5, a right model has been developed if its intended application is observed and confirmed by the experts. If the agreement is not acquired, the model will need to be amended to bring it closer with its intended application.

In Chapter 3, the theoretical foundation for the design and development of the new model was described (question 1); and in Chapter 4, the process of assessing whether the new model has achieved both utility and usability started through case scenario walk-throughs as well as a practical experimentation associated with this chapter which is discussed in detail in Appendix A (question 2). The guiding power of the new model emanates from the UML Activity Diagrams for different Processes of the CDFIPM as well as the model's Overriding Principles (question 3). However, the model now needs to be subjected to an evaluation of this guiding power that also extends the activities of Chapter 3 and 4 to establish whether the new model has both utility and usability (Adams, 2012). This evaluation will further determine whether the model has been developed right and whether the right model has been built (questions 4 and 5).

Therefore, the evaluation of the CDFIPM is the subject of this chapter and continues the Peffers et al's (2006) Design Science Research Process (DSRP), that requires the artefact to be used to address the research problem. The fifth step set out in the Peffers et al's (2006) DSRP, the Evaluation activity, requires the model to be validated in order to determine:

1. how well it supports the solution to the stated problem; and
2. whether it is necessary to iterate back to the step three (Design and Development) to try to improve the effectiveness of the artefact; or
3. whether it is needed to continue to the Communication activity (step 6 is discussed in Chapter 6) and leave further improvement to subsequent projects.

The remainder of this chapter is structured as follows: section 5.2 discusses the selected validation methods for the evaluation of the CDFIPM. Section 5.3 covers the process for expert selection, while section 5.4 describes the makeup of the expert panel. Section 5.5 discusses the process for communication with the experts and the acquisition of their feedback, while section 5.6 presents the evaluation questionnaire. The feedback analysis method is discussed in section 5.7. Section 5.8 discusses the analysis of the feedback and comments received by the reviewers, while section 5.9 presents the discussion of the evaluation. In section 5.10, alterations are made to the proposed model following the analysis of the acquired feedback, while section 5.11 refers the reader to the Appendix B for the final version of the proposed model. In section 5.12,

the proposed model is further assessed by subjecting it to the three sets of assessment criteria against which the previously proposed modes were judged in Chapter 2. In section 5.13, the proposed model is mapped to the previously proposed models. Finally, the chapter is summarized in Section 5.14.

5.2 Methods of Validation

Validation is the process of determining the extent to which an artefact (a model) and its related data are a correct representation of the real world from the standpoint of the intended applications of the model (Law, 2014). A set of validation methods can be employed to assess the model's accuracy in meeting its intended outcomes. There exist five main types of methods in relation to validating models or simulations including (Eddy et al., 2012):

1. Internal Validity – the model's components are analysed and their accuracy are checked;
2. Cross Validity – results are compared with other models analysing the same problem;
3. External Validity – model is used to simulate different scenarios;
4. Predictive Validity – model results are compared with prospectively observed events; and
5. Face Validity – independent experts evaluate the model structure, its associated data and results.

In the context of this research, methods 1, 2 and 3 above have already been applied to the CDFIPM in Chapters 3 and 4 (also see section 5.1). For instance, in terms of the Internal Validity method, the CDFIPM's components were analysed and justified in Chapter 3 (Design and Development), which addressed whether the CDFIPM's components behaved as intended and whether it had been implemented correctly. In relation to the Cross Validation method, the CDFIPM has been mapped and compared with the existing models in Table 3 (see section 5.13), which involves determining the degree to which they calculate the same results. With regards to the External Validation method, in Chapter 4 (Demonstration), the CDFIPM was applied to the different

scenarios and a walk-through of the model was performed to simulate different types of real life investigations.

Concerning method 4 above, Predictive Validity, this has been excluded from this research on the basis that this validation method will need to be carried out over a long period of time, during which it will involve employing the model to predict events and, after some time, comparing the predicted outcomes to the actual ones. Therefore, Predictive Validity has not been applied to the CDFIPM, being outside the timing scope of this research.

Face Validity (method 5), which is considered to be the strongest form of the 5 stated validation methods (Eddy et al., 2012; Law, 2014; Pace and Sheehan, 2002) is the topic of this chapter, where the external experts evaluate the model structure, its associated data, results and accuracy independently. This method is used to answer questions 3, 4 and 5 outlined in section 5.1:

3. Does the model provide explanatory or guiding power for the user?
4. Has the model been built right? and
5. Has the right model been built?

According to Pace and Sheehan (2002), the main validation method for models must include assessment by experts and peers. This argument is supported by other researchers in various scientific environments (Burgman et al., 2011; Czembor and Vesk 2009; Ludwig et al., 2001). Moreover, in circumstances in which empirical data are scarce or unobtainable[33], expert knowledge and their input are often considered to be the best or only source of information (Adams, 2012; McBride and Burgman, 2012; Kuhnert et al., 2010; Sutherland, 2006). In these situations, experts can be requested to provide input for all the stages of the modelling process (Martin et al., 2012; Cowling and Pressey 2003; Pearce et al. 2001). In all circumstances, the prevailing idea is to take advantage of the knowledge that cannot be acquired by relying upon other data sources and applying this knowledge to the evaluation of a model (Adams, 2012).

[33] Due to the fact that Digital Forensic Science is a new field, there exist little, if any, criteria against which a digital forensic process model process model can be evaluated against.

Thus, this chapter draws upon the Face Validity method by recruiting external independent experts to answer the remaining three questions and ultimately determine whether the CDFIPM has achieved both 'utility' and 'usability' necessary for a model.

5.3 Expert Selection Process

The process for selection of experts involved identification of the expertise that were relevant to the research aim and selection of the experts who would best meet the requirements for expertise within the thesis author's research timing scope. Booker and McNamara (2004) define the "Expert knowledge" as the knowledge and expertise that qualified persons have acquired due to their technical practices, training and experience. Based on this definition, it is, therefore, reasonable to regard an individual as a 'domain expert' if he/she is familiar with the subject at hand and is accountable for the analysis of the issue and provision of sound judgments.

Moreover, according to McBride and Burgman (2012), the experts should be selected on the basis of explicit criteria in order to ensure transparency and establish that the results represent the full range of views in expert field. The common metrics outlined in the literature for selecting experts include: experts' qualifications, employment, memberships in professional bodies, publication records, years of experience, peer nomination, and perceived standing in his/her community (Czembor and Vesk, 2009; Drescher et al., 2008; Whitfield et al., 2008). Additional considerations that need to be made include availability and willingness of experts to participate, and the possibility of conflicts of interest[34] (McBride and Burgman, 2012).

The appropriate number of experts should depend on (1) the scope of the research problem (see below) and (2) the available timing during which the research is expected to be completed (McBride and Burgman, 2012). However, the literature on expert selection strongly suggests the inclusion of as diverse a range of experts as possible (Armstrong, 2006; Clemen and Winkler, 1999) by recruiting multiple experts in order to reduce the impact of individual mistakes and biases and to pave the way for assessments that are representative of the entire expert community (Fisher, 2009; Hokstad et al., 1998).

[34] Experts who participated in the evaluation process did not know the thesis author.

In terms of the scope of this research problem, the research aim has three embedded aspects including:

1. 'being comprehensive' in that it encompasses the entire digital investigative process;
2. 'being formal' in that it synthesizes, harmonizes and extends the existing models and assists courts of law in determining the reliability of the digital investigative process followed; and
3. 'being generic' in that it is relevant to both law enforcement and corporate investigations.

In relation to the expert selection for the aspect 1 (being comprehensive), due to its many processes, the CDFIPM needed to be evaluated by different groups of experts with different sets of skills and expertise. For example, Digital Forensic Practitioners who often conduct the data acquisition were in the best position to provide a sound judgment on the CDFIPM's Acquisition Process. Similarly, Digital Forensic Analysts who often carry out the Examination, Analysis and Interpretation Processes were in the best position to comment on the corresponding Processes in the CDFIPM. Indeed, in most scientific environments as Martin et al. (2012) and Ludwig et al. (2001) point out, the breadth of research problems denotes that no one individual will be expert for all aspects of the problem. Hence, it was necessary to identify and recruit a diverse group of experts with different skill sets for the Evaluation process.

In terms of the expert selection for aspect 2 (being formal), it was deemed necessary to involve an appropriate and diverse set of experts such as legal practitioners in the Evaluation process.

With regards to the expert selection for aspect 3 (being generic), Ford and Sterman (1998), as cited by Adams (2012), emphasize the need to recruit expert knowledge from individuals who are routinely involved in the process. Therefore, since the CDFIPM is intended to be applicable to both law enforcement and corporate investigations, it was deemed necessary to recruit experts operating within the two stated fields to acquire expert knowledge for a practical evaluation of the CDFIPM. This approach would place the CDFIPM under both 'utility' and 'usability' testing (discussed in the previous

section) by the experts in relation to how 'useful' and 'relevant' the new model would be to each of the experts' particular domain of practice, and also with regards to how suitable the new model would be for describing the entire digital investigative process in each of the experts' particular fields.

Therefore, based upon the recommended common metrics as outlined in Czembor and Vesk (2009), Drescher et al. (2008) and Whitfield et al. (2008) (see the above), the following selection criteria were employed to identify and recruit experts who would be requested to evaluate the new model, the CDFIPM:

1. geographical operation – DFIs and legal practitioners would need to operate within the United Kingdom since the model is aimed at the U.K. jurisdiction.
2. period of experience and learning – the participants would need to have extensive knowledge and experience in the domain of digital forensics for a period greater than 10 years.
3. the manner in which the experience had been acquired – the experts' experience would need to have been attained through practice or theory in order to ensure that the expert panel would consist of both theorists and practitioners.
4. qualifications – the participants needed to have appropriate qualifications in relation to digital forensics, information security or computer science.
5. reputation – the experts would need to have a solid standing in their particular domains of practice.

Having rationalized the expert selection process and identified the criteria for such a selection, the next section expands upon the constituents of the selected expert panel.

5.4 Expert Panel Makeup

In order to address the research aim, a diverse set of eminent experts within the U.K. jurisdiction were identified and recruited to review the new model and provide their feedback. Recruiting numerous experts to evaluate the CDFIPM was considered to be a necessary approach in order to acquire the needed expert coverage even though this was

not a straightforward process[35]. The use of this diverse set of experts was deemed to be beneficial to increase what McBride and Burgman (2012) label as "the acceptance or perceived validity of the elicitation process". The recruitment of a varied set of experts would ensure that different perspectives would be brought into the Evaluation process.

Experts who took part in the evaluation of the CDFIPM were categorized into three groups of:

1. Digital Forensic Investigators (DFIs)[36];
2. Legal Practitioners; and
3. Academics.

Experts from the panel were identified as representative of their specific domains of practice based on their roles, responsibilities, experience and involvement within pertinent associations within the U.K. jurisdiction. The recruitment process for the expert panel was considered complete once numerous participants from each of the three fields covered by the research scope had consented to assist. The followings are the profiles of the experts constituting the members of the three groups of the expert panel:

1. **A representative of law enforcement who:**
    - manages the entire High-Tech/Cyber Crime team of North West Regional Organised Crime Unit (TITAN), consisting of six police forces in Cumbria, Cheshire, Lancashire, Greater Manchester, Merseyside and North Wales;
    - is a Detective Sergeant of e-Forensics with 25 years of experience as a police officer, 15 years of which as a digital forensic investigator;
    - is a sub-contracted Technical Assessor for UKAS (United Kingdom Accreditation Service) as an ISO 17025 Forensic Laboratory Auditor and ISO 17025 Technical Assessor; and

[35] Selection of the appropriate experts who could provide valuable input to this research was a very long and enduring experience involving a period of over 9 months and travelling across the country which would sometimes result in disappointments as some potential participants would pull out at the last minute due to the workload or their lack of availability.

[36] This refers to Digital Forensic Practitioners, Digital Forensic Examiners, Digital Forensic Analysts, Case Officers and Digital Forensic First Responders.

- has an MSc in Computing & Information Technology and is EnCase Certified Examiner.

2. **A representative of commercial practice who:**
    - is the director of Digital Forensics for a large company (based in Nottingham) providing digital forensic consultancy services;
    - has 18 years of experience as a Digital Forensic Investigator and a Forensic Triage Specialist;
    - has previously managed the Nottinghamshire Police High-Tech Crime Unit as a Detective Sergeant both in Digital Forensics Unit and also in Fraud Squad; and
    - is on the editorial panel for the ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation and the ACPO Good Practice Guide for Digital Evidence.

3. **A representative of legal practice who:**
    - is a self-employed barrister with 13 years of experience;
    - practices in Criminal Law from Apex Chambers, based in Cardiff;
    - has worked on over 20 cases involving digital investigations;
    - has an LL.B; and
    - has acted as an external examiner within the University of West England.

4. **A representative of law enforcement who:**
    - heads the Cheshire Police Headquarter (Cheshire Constabulary) High-Tech Crime Unit;
    - is a Detective Sergeant of eForensics with 28 years of experience as a police officer, 14 years of which as a Digital and Network Forensic Investigator; and
    - has a BSc in Computing and Information Technology and is a certified ENCE, a certified Security Incident Specialist, a certified Forensic Investigation Analyst and a qualified force trainer for eForensics.

5. **A representative of commercial practice who:**
    - is the Chief Technical Officer (CTO) in a large company (based in London) providing IT services including Digital Forensics;
    - has 30 years of experience in Information Technology; and
    - has an MPhil in Operating System Anti-Malware/Security and an MSc in Internet Engineering.

6. **A representative of law enforcement who:**
    - is a Detective Constable of Digital Forensic at the South Wales Gwent Police High-Tech Crime Unit; and
    - has 18 years of experience as a police officer, 11 years of which as a Digital Forensic Investigator.

7. **A representative of law enforcement who:**
    - is a Detective Constable of Digital Forensic at the South Wales Gwent Police High-Tech Crime Unit; and
    - has 11 years of experience as a Digital Forensic Investigator.

8. **A representative of Academia who:**
    - is a university professor and a prominent researcher with many publications on information security, biometrics and digital forensics;
    - has a PhD and the title of "professor"; and
    - is the key note speaker at reputable information security and digital forensics conferences.

9. **A representative of legal practice who:**
    - is a Deputy High Court Judge and a barrister based in Exchange Chambers within Manchester, Leeds and Liverpool;
    - has 34 years of experience of practicing law;
    - is current Chairman of the Northern Chancery Bar Association and is a Trustee of the North West Partnership;
    - practices criminal law with the main focus on commercial fraud; and
    - has an LL.B.

10. A representative of Academia who:

- is a university professor and a well-known researcher with various publications on digital forensic practice; and
- has a PhD and has extensive links with the industry

Having discussed the constituents of the selected expert panel, the next section discusses the format of communications with these experts and the way in which the feedback was acquired from the expert panel.

5.5 Communication and Feedback Formats

In the first instance, the participating experts in the Evaluation process were requested to assist in this research via email. The experts were identified as being representatives of their specific domains of operation based on their roles, responsibilities and involvement with relevant associations. After the experts were identified and their confirmation for participation in the Evaluation process was obtained, then in line with the best practices outlined in the literature (Rothlisberger et al., 2010; Cooke and Goossens 2000; Morgan and Henrion, 2010), they were provided with relevant materials associated with the CDFIPM that had been compiled into an appropriate, accessible form. These consisted of the UML Activity Diagrams of the CDFIPM's Processes, the explanatory notes based on the descriptions of the model's components, a questionnaire, background information such as the aim and objectives of the research, and also a description of what the thesis author requested the experts to undertake. These materials were sent to the participating experts via email so that they could have sufficient time to evaluate them, raise any potential concerns, comment on any aspect of the model, and volunteer relevant information. Having acquired the expert knowledge (data) via e-mails, the thesis author would then hold formal meetings with the experts in the form of interviews and focus groups (see the end of this section) in their work environments for further knowledge extraction process.

In terms of the provided questionnaire, based on the utility and usability testing (Adams, 2012), experts from the panel were requested to review typical tasks pertaining to those stages of the investigative process that were relevant to their own domains

through using the CDFIPM, and then to provide a subjective rating on the basis of how 'useful' the model would be to their domains of practice, and also how 'easy' it would be to use the new model (see the Evaluation questionnaire in section 5.6). This subjective rating was to be taken into account in order to enhance the model. Prior to submitting the materials to the experts for eliciting their knowledge, these were carefully piloted (tested and revised) to ensure that the documentations had been compiled properly. It was important to ensure that the Evaluation questions had been formulated appropriately to reflect the research aim and objectives, identify potential issues with biases or question phrasing, and receive feedback about any potential ways to enhance the quality of the process and of the knowledge that was to be extracted. The pilot process was conducted with the thesis author's director of study and supervisor, who checked the compiled documents prior to them being submitted to the experts for review. As stated above, once the initial feedback was acquired from the experts via e-mail communications, the thesis author would then travel to the experts' workplaces at an arranged date to discuss their feedback with them and to elicit further expert knowledge that was not possible to obtain via e-mails. These meetings would take place through focus group and interview formats. Such an approach is recommended in the literature based on its advantages as follows (Ciardhuáin, 2004):

- The interview and focus group format take full advantage of the experience and skills of those participating by being more open than a narrowly-focused survey.
- Experts have a stronger understanding of the subject matter as they can ask questions concerning the research than simply replying to a fixed set of questions.
- Participants are able to express and discuss views that are very likely not to be identified by a simple survey. Such issues can be analysed at once in some detail.
- Experts are left free to express their views in whatever manner they feel is most appropriate.

Having discussed the formats of communication and expert knowledge elicitation process, this discussion continues to the next section, where the questionnaire submitted to the expert panel will be presented.

5.6 Evaluation Questionnaire

The following is the questionnaire consisting of a set of 8 questions that was submitted to the expert panel as part of the Evaluation process. In addition to this set of 8 questions, there was an additional question which was posed only to the legal practitioners in order to elicit the knowledge that was necessary to be acquired in relation to answering the second aspect of the research aim, which is:

> *The CDFIPM must be formal in that it assists courts of law in determining the reliability of the digital investigative process followed.*

This question is as follow:

> *If this model were explained to you by a digital forensic investigator who has employed it to conduct a digital investigation, as a judge/barrister, do you think that the model would enable you easily to understand the steps taken by investigators to acquire digital evidence? If so, can you explain how?*

The Comprehensive Digital Forensic Investigation Process Model (CDFIPM)

Please notice: any personal information provided will be kept confidential and will be deleted once the comments and feedback have been reviewed and analysed.

Prior proceeding to the questions, please state:

Your full name: _____

The institution you work/ have worked for: _____

Your job titles related to domain of digital forensics: _____

Your period of learning and experience: _____

The condition in which the experience has been gained: _____

In reviewing / evaluating the model:

1. Please identify any aspects of the model that are not representative of the processes as carried out in your field of practice (utility).

2. Please identify any aspects of the processes carried out in your field of practice that are not covered in this model (utility).

3. Did you think that the model adequately represented the structure of investigations in your organisation (utility)?

4. Please describe which activities in the model most closely relate to your field of practice and your own experience (utility).

5. Please describe what aspects, if any, of the model you felt could be improved (utility).

6. Please rate the model on the scale of 1 to 10 with 1 not being useful at all and 10 being the most useful (utility).

7. Please rate the model on the scale of 1 to 10 with 1 being very difficult to use and 10 being very easy to use (usability).

8. Please provide any additional comments that you might have on the model attached.

(Please provide your answers/feedbacks/comments on a separate sheet of paper.)

Figure 41. Evaluation Questionnaire

5.7 Feedback Analysis Method

After the elicitation process was completed, the expert knowledge acquired (data) was analysed through a rigorous verification process. In line with McBride and Burgman's (2012) and Cooke's (1991) suggestions, during the process of data analysis, the thesis author checked for obvious errors or inconsistencies by comparing the expert's responses to those of others in the panel. In comparing an individual expert's responses with those of the rest of the panel, the thesis author looked for similarities, irregularities, biases, or strongly conflicting opinions in addition to varying interpretation of the information. When such irregularities or problematic responses were identified, the thesis author followed up on the conflicting feedback through further discussions with the experts. As an example, DFIs operating within both Cheshire and Gwent Police HTCUs stated that the suspect must be interviewed at the crime scene, whereas one of the legal practitioners (barrister) based in South Wales refused such a notion on the basis of tight U.K. laws. In this situation, the thesis author had to follow up the conflicting response to bring clarity to the feedback. The aim of the verification aspect of the analysis process was to reach a final set of judgments that the expert panel had approved and to ensure that the documented responses were reliable and that they would truly and faithfully reflect each expert's true beliefs.

5.8 Expert Feedback and Analysis

After collecting the feedback from the expert panel via e-mails, focus groups and interviews, hereafter referred to as the 'Feedback Elicitation Formats', these feedbacks were analysed and acted upon where necessary. The feedback, comments and views expressed by the experts were both very positive and promising. The aim of this section is to provide a subjective analysis of these feedbacks. In order to do so, these feedbacks are presented in the form of quotes derived from the Feedback Elicitation Formats together with the thesis author's specific comments in response to these detailed feedbacks. Acting upon the acquired feedback will involve 'addition to', 'alteration to' and 'deletion from' the CDFIPM. 'Addition' refers to a new component being added to the model, 'alteration' refers to the change in a component's naming or order and 'deletion' refers to the deletion of a component from the model. Therefore, those

feedbacks that the thesis author has acted upon by making an 'addition to', 'alteration to' or 'deletion from' the model will be represented by the following three types of references (The idea of the following format is derived from Adams' (2012) study):

1. **Reference to Addition:** 'REF: ADD #n', where 'n' represents the number of implemented 'addition'.

2. **Reference to Alteration:** 'REF: ALT #n', where 'n' represents the number of implemented 'change'.

3. **Reference to Deletion:** 'REF: DEL #n', where 'n' represents the number of implemented 'deletion'.

Prior to discussing the detailed feedback acquired from the experts and the analysis of those feedbacks, some positive general comments made by the expert panel in relation to the CDFIPM are first presented in the next sub-section.

Notice: The evidence of both general positive feedback as well as detailed feedback will be provided as audio recordings as well as e-mail printouts upon a request.

5.8.1 General Comments from the Expert Panel

- *"I can see a lot of work has been put into this and you have covered everything I can think of, my only comment would be enabling your model to be interactive rather that a set procedure." (Law enforcement DFI and Case Officer)*

- *"The model is impressive in its detail and reasonably easy to understand and use. The author has clearly understood the practicalities of an effective and efficient digital investigation." (Legal practitioner, barrister)*

- *"With ACPO Guidelines, there is no defined structure to it, no defined path to it. What we need is that these methods have been validated scientifically. This is something you have worked out over long time. Your model has been peer*

reviewed both by practitioners and scientists even though we might choose it differently." (Law enforcement DFI)

- *"This model is very timely and well-researched. It is my conclusion that you have gone deep enough into details of finding out what exactly is wrong with the existing models and what to do to improve them." (University professor)*

- *"This is sound standard for forensic service providers (FSPs). This is like UCAS was." (Law enforcement DFI)*

- *"Your model provides a concise guidance on the exact processes that examiners need to follow during any kind of digital investigation." (Commercial DFI)*

- *"It is necessary that the court understands the process that has been followed. Your model has done a great job as its processes are documented in a very rational way. A judge or barrister could pick up this model and work out what has been happening in a digital investigation." (Legal practitioner, judge)*

- *"What you have presented is actually good. You have done a great job; I feel that the model you have presented would accelerate digital investigations because it gives a common order of processes and activities that a computer forensic investigation requires." (Law enforcement DFI and Case Officer)*

- *"Your model is like modular plugin type for different fields." (Law enforcement DFI)*

- *"There is much in your model that covers cybercrime and such attacks that are not covered in LE." (Law enforcement DFI)*

- *"Sorry for the delay in replying. I have had a chance to look at your model and it is sound in its interpretation. How would you like my feedback?" (Commercial DFI)*

- *"Your model reflects in part our Cheshire's existing model, and I do not intend changing to anything other in the near future as this model simply reflects what we already have." (Law enforcement DFI and Case Officer)*

- *"I have had an initial look at your work and it looks interesting and a very comprehensive model." (Commercial DFI)*

5.8.2 Detailed Feedback and Response

Feedback E-1: *Readiness and Incident Detection are not part of Cheshire's model. We rely more heavily on intelligence.*

- **Response:** Considering the fact that the above comment was made from a law enforcement perspective, this was expected as the two Processes are often carried out in the commercial practice. Hence, this is why they had been developed as part of the CDFIPM to accommodate also for corporate requirements. Incident Detection in the context of law enforcement often comes in the form of a '101' or '999' call, or 'intelligence' (see the next feedback 'Feedback E-2') such as witnesses or the suspect's spouse.

Feedback E-2: *We rely heavily on intelligence as part of crime detection and also our planning activities. It would be important to include activities related to intelligence gathering in your model. Add an additional stage between 'incident detection' and 'planning' in the model.*

- **Response:** This is an important aspect of an investigative process often carried out within the law enforcement environments that had not been previously included in the CDFIPM. A new Process entitled Intelligence Gathering will now be added to the model so that its results feed into the Planning Process of the CDFIPM. Based on this new Process, DFIs will be

required to collect intelligence using both covert (on condition that the authorisation permits its doing so) and overt methods. Moreover, they will also need to assess the acquired intelligence, profile suspects and formulate initial hypothesis during this Process. ("REF: ADD #1")

Feedback E-3: *Event Reconstruction is something we do not tend to practice as it is labour intensive. However, I would use this if the circumstances dictate.*

- **Response:** The above feedback is arguable. Although Event Reconstruction might be labour-intensive, it still must be part of any digital investigation so that it, together with the Analysis and Interpretation Processes, can enable DFIs to construct a full picture of the events that have taken place. If DFIs do not perform the Event Reconstruction Process, questions in relation to who, why, where, when and how will not be addressed properly. As a result, this can severely affect the outcome of the case in courts. However, in certain circumstances, Event Reconstruction might not be as necessary; for example, when the incident/crime is not classified as severe, and the investigation results are to be presented to the company management as opposed to a court. Thus, no further action will be taken in light of the above feedback.

Feedback E-4: *We perform an on-scene triage (Triage stage 1) to determine evidential possibilities and opportunities as soon as possible. We then perform a Stage 2 (secondary triage) back at the lab and this could be the same day.*

- **Response:** Onsite Triage is a major aspect of an investigative process which is carried out especially in law enforcement investigations that had been excluded from the CDFIPM. Both Cheshire Police and Gwent Police HTCUs underlined the importance of Onsite Triage to the law enforcement digital forensic investigations. Due to the rapid increase of digital based

evidence, DFIs will need to perform timely identification, examination and interpretation of digital evidence. Also, in certain investigations such as child abductions, pedophiles, missing or exploited persons, time becomes extremely important as in some cases, it is the difference between life and death for the victim. Moreover, the growing number of computer systems being submitted to DFLs is creating a backlog of cases that can delay investigations and negatively affect public safety and the criminal justice system. Therefore, it was deemed important to act upon the above feedback and include steps for Onsite Triage in the amended form of the CDFIPM. This is to enable DFIs to acquire information in a timely manner, and also to avoid backlog of cases by reducing the number of computer systems submitted to DFLs for analysis[37] [38]. ("REF: ADD #2")

In terms of the Stage 2 Triage (Offsite Triage), implementing components for this is outside the scope of this thesis as this should be part of any HTCU's Standard Operating Procedures (SOPs), where the HTCU implements some methods (e.g. based on a matrix system) for determining the worth of a case prior to its acceptance for investigation as well as rating the emergency of and prioritising the accepted case. Moreover, the topic of Offsite Triage has already been covered; for example, see Parsonage (2009).

Feedback E-5: *Risk assessment should be treated as a principle throughout the whole process; it is important that you keep assessing the risks continually.*

- **Response:** An Overriding Principles, namely 'Perform Risk Assessment', will be added to the CDFIPM's Concurrent Processes Class that must be performed throughout the entire investigative process. ("REF: ADD #3")

[37] Adding Onsite Triage to the CDFIPM will assist DFIs in determining (at the crime scene) whether the digital system under investigation contains any potential evidence in the first place prior to seizing the device.
[38] For more information on "Onsite Triage", see a journal paper by the thesis author in Montasari (2016, b).

Feedback E-6: *Most of our planning and preparation (important) is done in advance prior to our first response in attending the scene. As a result, the target is known and is assessed along with the premises. All equipment is ready to go in advance, so we go from preparation of equipment, processes and people attending and planning prior to first response.*

- **Response:** The comment above is not misguided since the concept behind it is valid. As the expert has correctly pointed out and this had also already been explicitly explained in Chapter 4, Planning and Preparation Processes must always be carried out prior to DFIs launching the First Response Process. The above comment is essentially requesting the change in the order of Processes where Planning and Preparation must be placed before the First Response process. However, the two stated Processes (Planning and Preparation) had already been placed before the Secure and Evaluate the Crime Scene Process, which was intended to be the First Response in the context of 'law enforcement' investigations. There are two Processes in the CDFIPM that refer to the First Response. The first Process which is explicitly entitled First Response was intended to be used in the context of 'corporate investigations', while the second Process that is entitled Secure and Evaluate the Crime Scene was intended to be employed in the context of 'law enforcement'.

  The above feedback might therefore be explained by the fact that the expert has seen the two stated Processes (Planning and Preparation) immediately after the first 'First Response Process' and assumed that the Planning and Preparation Processes have been placed in the wrong order. This issue was raised by other experts (see Feedbacks E-7, E-18 and E-19) which resulted in the thesis author contacting both experts again for clarification. Having held further discussions with the experts, it became obvious that the terminology had caused such a confusion. Both experts suggested removing the first "First Response" Process as it has exact the same components as the Secure and Evaluate the Crime Scene and changing the naming of the latter to the 'First Response', which now becomes a generic process for both law

enforcement and corporate investigations. ("REF: DEL #1") and ("REF: ALT #1")

Feedback E-7: *Planning should be before first response and likewise some companies will constantly plan for an attack and frequently test their methods/tools in advance so when an incident does occur the plan is already in place as to what to do, so all staff know their role in reducing risk and dealing with it in response to a threat.*

- **Response:** See Feedback E-6 in relation to the ordering of the Planning, Preparation and First Response Processes. In terms of determining personnel, their roles, responsibilities and skills, these had already been explicitly incorporated into the CDFIPM's Planning Process as Sub-Phases under the Plan Logistic Phase (see Figure 26). Also, in relation to preparing and testing tools and techniques, this had already been clearly incorporated into the CDFIPM's Concurrent Processes Class as one of the Overriding Principles. It appears that the expert has missed observing the inclusion of the aforementioned components in the CDFIPM. Therefore, no action will be taken in light of the above comment.

Feedback E-8: *You have quoted a number of ISO Standards but take a look at ISO 17025 that comes into play this year that we are seeking accreditation for.*

- **Response:** At the time of writing (June 2016), ISO 17025 is still under development and is intended to be released within the next few months (seemingly next 18 months). This Standard highlights some general requirements for DFLs to carry out tests in relation to their tools and methods including sampling. As both Detective Constable Tim Williams and Detective Constable Mark Maybiy from the Gwent Police HTCU stated, all the UK Police Forces' HTCUs will still need to have a digital forensic

investigative model in place that ISO 17025 fits in with. Both DFIs stated, "we (HTCUs) will still need to define our investigative processes such as your model that would need to fit in with the ISO 17025."

Feedback E-9: *Safety issue regarding both individuals and equipment is something that you should address throughout the whole investigation.*

- **Response:** An Overriding Principles entitled 'Address Safety Issues' will now be added to the CDFIPM's Concurrent Processes Class that will need to be performed concurrently throughout the entire investigative process. ("REF: ADD #4")

Feedback E-10: *As regards to the terminology, some stages are too broad or vague, or too technical, and further guidance and detail would be useful.*

- **Response:** See the Feedback E-11 and Feedback E-24.

Feedback E-11: *Have a key for phrases that may not be familiar to the user. A 'key' often appears as an endnote at the end of a document or a footnote at the end of a page so that terms unfamiliar to the user can be explained without taking up room in the main body of the document.*

- **Response:** This comment is similar to the view expressed by the expert in Feedback E-10. Although this feedback is valid, this must be carried out by the individual who prepares the forensic report (often Digital Forensic Analyst) to be presented to a court or the company management. This can easily be addressed by providing supporting explanations for difficult and

technical terms as a 'Glossary of Terms' in one of the appendices of the forensic report. This has been demonstrated in the Appendix A of this thesis as part of the practical experimentation of the research (a hypothetical digital crime and its investigation).

Feedback E-12: *Further planning on site is common place (splitting room to exhibit locations for instance) and what we decide to triage on site or seize depends on what we are faced with.*

- **Response:** 'Further planning" at the crime scene had already been explicitly incorporated into the CDFIPM's Planning Process as a Phase entitled 'Update the Outline Plan'. Thus, no additional action will be taken in this regard. In terms of the point regarding Onsite Triage that the expert has raised, since the need for Onsite Triage was pointed out by another expert, steps for Onsite Triage will be added to the CDFIPM as stated in 'Feedback E-4'. ("REF: ADD #2")

Feedback E-13: *Assess risks – state the most common examples as a prompt.*

- **Response:** The above comment is referring to the Perform Risk Assessment Phase included in the CDFIPM's Planning Process. Although this is a valid operational point, it is too specific for inclusion into a generic process model. Therefore, no action will be taken in this regard as assessing risks should be specific to an investigation at hand and must be carried out by the person in charge of the investigation (often Case Officer) based on the SOPs of the investigating organisation. Moreover, two generic Sub-Phases, namely Assess Risks Related to Original Media and Evidence and Assess Risks Associated with the Personnel, had already been included under this Phase.

Feedback E-14: *'Describe incident' should come before 'classify incident'.*

- **Response:** The above comment is aimed at Describe Incident and Classify Incident Phases included in the CDFIPM's Incident Detection Process. This feedback is relevant as incident needs to be described before it can be categorised. Thus, the ordering will be amended. ("REF: ALT #2")

Feedback E-15: *You wouldn't interview the suspect at the crime scene.*

- **Response:** This view was expressed by a legal practitioner (barrister) which initially appeared to be in contradiction with the approach that the law enforcement officers had advised the thesis author they would take, as well as the thesis author's own research under sub-section 3.7.1.3 of Chapter 3. From the legal practitioners' point of view, the laws associated with interviewing suspects at the crime scene are strict and must therefore be adhered to stringently. Due to the conflicting opinions, further discussions took place between the thesis author and the legal practitioner prior to approaching the law enforcement DFIs again to seek their advice and have the opposing opinions clarified. The followings are brief extracts of the conversation between the thesis author and the legal practitioner:

  The thesis author: *"In terms of saying that suspects are not interviewed at the crime scene, does this also apply to severe situations when a person is missing and quick information is required, when life is in danger, or when the investigation involves a missing child or child pornography? If the officers present the suspect with incriminating evidence to encourage him to talk, is this unlawful? When I met up with the officers from both the Cheshire Police Headquarter and Gwent Police HTCUs, they informed me that sometimes suspects, themselves, would own up to what they have done because the evidence is compelling. So, could you please advise me on this conflicting issue further?"*

The barrister: *"It does not generally happen. If the police have enough information, they must charge the suspect, at which point there are extreme rules about when and how they can question them – there are lengthy Codes of Conduct about it. If they do not yet have enough information, they can of course ask questions. If you can, check with your police officer what they would do in the scenarios you present, such as a missing person or where life is in danger – I'm afraid I don't have a definite answer in relation to that."*

Upon further discussions with the law enforcement officers from both aforementioned police forces, once again they confirmed that it was completely acceptable to question suspects at the crime scene in severe situations as mentioned. Therefore, Interview the Suspect Phase will not be removed from the model, and the investigating organisations who would follow the CDFIPM must apply this phase when conducting digital investigations.

Feedback E-16: *'Document the crime scene' – does this need to be under a different arrow?*

- **Response:** This comment is referring to the Document the Scene Phase included in the Secure and Evaluate the Crime Scene Process. The fact that this Phase has been placed under a different arrow (which refers to a UML Activity Diagram graphical notation) indicates that this phase must be performed in parallel throughout all the other phases in this Process. Thus, no action will be taken in this regard.

Feedback E-17: *Have 'organise' then 'classify' rather than having them running in parallel*

- **Response:** This will be amended. ("REF: ALT #3")

Feedback E-18: *How do you 'secure crime scene' in First Response without attending the site, which appears for the first time in 'Secure and Evaluate Crime Scene' section?*

- **Response:** As stated in Feedback E-6, having both First Response and Secure and Evaluate the Crime Scene Processes created some confusions for a number of experts and drew valid criticisms. As also stated, First Response Process will be removed from the CDFIPM and the Secure and Evaluate the Crime Scene Process will be renamed to First Response. ("REF: DEL #1") and ("REF: ALT #1")

Feedback E-19: *How is 'Preserve and Secure Physical Crime Scene' different from 'secure crime scene'?*

- **Response:** the above question raised by one of the experts again pertains to the confusion caused by the first 'First Response Process' in the CDFIPM. This feedback is referring to two of the Phases within the First Response Process that have appeared to the expert to be repetitive. As stated in Feedback E-6, this issue will be addressed automatically by removing the first 'First Response' Process from the model and renaming the 'Secure and Evaluate the Crime Scene' Process to 'First Response'. ("REF: DEL #1") and ("REF: ALT #1")

Feedback E-20: *There should be an activity in the final stage of the model (Future Readiness) that will require the examiners to enter feedback as part of a knowledge-building process to help any future incident?*

- **Response:** this activity had already been covered under a different terminology, namely Make Recommendations, as a phase within the Future Readiness Process. Therefore, no further action will be taken in this regard.

Feedback E-21: *Include team/investigation debrief in the investigation closure section.*

- **Response:** this had already been covered under a different terminology 'Conduct a Critical Review' in the CDFIPM's Investigation Closure Process. Since it appears that DFIs are more accustomed to the term 'debriefing' as this was pointed out also by a number of different experts, the naming 'Conduct a Critical Review' will now be changed to Conduct a Team/Investigation Debrief. ("REF: ALT #4")

Feedback E-22: *How is 'Identification' different from what has gone before?*

- **Response:** This is an important point which was appropriately raised in relation to two of the Phases of the Identification Process, namely Search and Identify, that had already been covered as two sub-phases under the Carry out Preliminary Survey Phase of the Secure and Evaluate the Crime Scene Process. Therefore, the Search and Identify Phases of the Identification Process will be removed on the basis of their repetitions in the preceding Process. ("REF: DEL #2")

  At this stage, it appears that the Identification Process will be left with only one remaining phase, namely Prioritize. However, since it has already been determined to subject the Secure and Evaluate the Crime Scene Process to new additions in terms of Onsite Triage and Prioritization based on the 'Feedback: E-4 ("REF: ADD #2")', the Prioritize Phase will also become redundant in the Identification Process. Therefore, the entire Identification Process will be removed from the CDFIPM. ("REF: DEL #3")

Feedback E-23: *'analysis' should come before 'developing hypothesis'. Although having analysis + hypothesis would be sufficient, you could always have a re-analysis in light of the hypothesis afterwards. In reality a competent investigator would always re-evaluate; so*

having a 're-analysis' component would simply acknowledge that (& perhaps encourage / remind less competent investigators to do so!)

- **Response:** The above feedback is aimed at Develop a Hypothesis and Analyse Digital Evidence Phases of the Analysis Process. The ordering of the two Phases will now be changed and a new Phase entitled 'Reanalyse Digital Evidence' will be included after Develop a Hypothesis Phase in the Analysis Process. ("REF: ALT #5") and ("REF: ADD #6")

Feedback E-24: *What is meant by 'reduce acquired data'? Why?*

- **Response:** The above question was posed by a legal practitioner in relation to the Reduce Acquired Data Phase of the Examination Process. The following is the response that the thesis author provided and the legal practitioner's further feedback.

  Thesis author: "*In terms of the 'Reduce Acquired Data' Phase, since a digital device can contain a large amount of data, most of which are not related to the case under investigation, investigators will therefore need to reduce data only to what they are interested in. Does this make sense?"*

  The legal practitioner: "*Yes, that makes sense. However, the fact that I (as a lay person) had to ask suggests it may be useful to provide a better explanation. An option would be to have a 'Glossary of Terms' at the end of the document – I think that would be really valuable, and I have seen them used a lot in other technical documents presented to the court."*

  This issue was also raised in Feedbacks E-10 and E-11 and addressed in Feedback E-11.

Feedback E-25: *There is no need to have 'Consolidate investigation findings' when you have 'review investigation results' immediately after it.*

- **Response:** Consolidate Investigation Findings Phase will now be removed from the Event Reconstruction Process as it appears to be repetitive to its following Phase, namely Review Investigation Results. ("REF: DEL #4")

Feedback E-26: *After 'Identify areas of improvement', have a further action to act on any areas identified.*

- **Response:** A new Phase entitled 'Act upon Any Areas Identified' will be added after Identify Areas of Improvement (if any) Phase of the Event Reconstruction Process. ("REF: ADD #7")

Feedback E-27: *In the 'Presentation' section, why is there a requirement to consider the appeal process at this stage?*

- **Response:** The Consider Appeal Process had been included in the Presentation Process in order to enable the investigators to make contingency plans in advance to take account of possible case rejection by courts of law where they would need to launch an appeal. Therefore, this Phase will remain in the Presentation Process, and no further action will be taken.

Feedback E-28: *Consider re-ordering 'Presentation' section as follows: Determine the target audience – Understand the requirements of the presentation – Consider (and apply) the legal jurisdictional requirements – Consider the appeal process – Prepare exhibits – Use appropriate presentation aids – Present the report – Prove/ defend the validity of the hypothesis – Decide the case*

- **Response:** The ordering of the Phases in the Presentation Process will be amended as suggested above. ("REF: ALT #6")

Feedback E-29: *In 'Investigation Closure' section, 'Record the case decision' should come after accepting or rejecting the hypothesis and before the question of whether the evidence can be returned.*

- **Response:** The Record the Case Decision will now be placed immediately after the Accept or Reject the Hypothesis Phase as suggested in this feedback. ("REF: ALT #7")

Feedback E-30: *If the evidence cannot be returned, have separate actions for (a) store, cleanse and re-use the evidence, and for (b) destroying the evidence – ask a question the answer to which would identify which of these 2 options would be followed.*

- **Response:** The above comment refers to the management of evidence in the Investigation Closure Process. This is a very constructive feedback which was brought to the thesis author's attention as no explicit condition (question in the form of UML Activity Diagram notation) had previously been specified with regards to the sensitivity of digital evidence. Further clarification was needed in terms of the legal aspect of sensitive digital evidence. Therefore, further communication took place between the thesis author and the legal practitioner (judge) as follows:

  Thesis author: "*Thank you very much for bringing such an important issue to my attention. I am going to create further condition as suggested. So, this will be like this: 'Can the evidence be returned?' If the answer is 'yes', the evidence will be returned. If the answer is 'no', the investigator will be provided with another condition asking whether the evidence can be destroyed. If the answer to this question is 'yes', the investigator will need*

to destroy the evidence. If the answer is 'no', the investigator could cleanse and reuse the device. From a legal point of view, is this a sound approach? And is this similar to what you thought?"

Judge: "*Yes. I don't know whether you also need to include a more detailed guide for the investigator as to when each step would be appropriate. For example, presumably 'sensitive' information would not be returned, but would be destroyed. It may help investigators to have a finite list of which types of evidence would fall into each category; but I don't know if this goes beyond the remit of what you are trying to achieve here. Another, perhaps simpler way might be this:*

- *'Is the evidence sensitive?' (And / or other terms that would cover all scenarios which you would decide whether to return, destroy or cleanse & reuse evidence.)*
- *Yes – it cannot be returned – Can it be destroyed? ……. (Cleanse and reuse, etc.)*
- *No – it can be returned.*

Based upon the above detailed feedback and further clarification, three new conditions have been developed that will be included in the Presentation Process to accommodate also for 'sensitivity' of digital evidence ("REF: Add #8"). However, developing a fixed list of which types of evidence would fall into each category is outside the scope of this research and must be determined by the investigating organisations based on their own internal guidelines.

Feedback E-31: *Consider swapping order of 'make recommendations' and 'develop a case study' in 'Future Readiness".*

- **Response:** The ordering will be amended. ("REF: ALT #8")

5.9 Discussion of Evaluation

The aim of this chapter was to evaluate the CDFIPM further in order to determine whether it has achieved both components of 'utility' and 'usability'. To this end, five questions were raised that needed to be addressed. It was established that the first three questions out of the five had already been answered throughout Chapter 4 and 5. However, to address the remaining questions four and five ("has the model been built right?" and "has the right model been built?"), the model needed to be subjected to an independent, external evaluation that would extend the activities of Chapter 4 and 5. Therefore, the topic of this section pertains to the utility and usability of the CDFIPM to determine answers to the remaining two questions.

5.9.1 Utility

The 'utility' component of the Evaluation activity was intended to ensure that the CDFIPM has 'serviceability', 'applicability' and 'appropriateness' to the law enforcement, commerce, incident response and legal domains as stated in the research aim. The CDFIPM was therefore subjected to an external, independent evaluation by the leading experts in its intended user community to ensure that it had captured the entire investigative process as carried out by experts in the stated fields. The comments regarding the CDFIPM were very positive, and the feedback was both constructive and insightful. There were a total number of 31 detailed feedback including suggestions for new additions, amendments and deletions. Out of the 31 feedback, 8 new additions, 8 amendments and 4 deletions were made into and from the CDFIPM. Having made the new model subject to experts' scrutiny, it became clear that there did not exist any aspects of the CDFIPM that were not representative of the processes as carried out in the fields covered by the research scope. Similarly, there were not any aspects of the processes as performed in the stated fields that were not covered in the CDFIPM.

In response to the question of utility (see the questionnaire in section 5.6), "Please rate the model on the scale of 1 to 10, with 1 being not useful at all and 10 being the most useful.", experts provided the mean score of '9'. This suggests that the CDFIPM has achieved its intended component of utility required of a useful artefact. The followings are some comments made by experts in relation to the utility of the CDFIPM:

- *"Much of your model covers most aspects in good detail of what is required but the order would change or be adopted to operational needs. But, all principles and processes are there in good details." (Law enforcement DFI and manager)*

- *"You have identified the relevant problems with the current models and have provided detailed analysis. I believe that your model has made a significantly novel contribution in its current length and presentation. Congratulations on accomplishing such a daunting task!" (University professor)*

- *"This model allows a smooth transition from one phase to another during a digital investigation. If I were to use it, it would certainly give me a detailed advice about what to do with the evidence." (Commercial DFI)*

- *"You have covered all avenues in different elements of digital investigations." (Law enforcement DFI)*

- *"It is absolutely practicable and structured. You would not go wrong." (commercial DFI)*

- *"This model is very comprehensive; I can't see any loopholes. Some issues are raised about detaining a suspect, where there could be multiple persons in a property with none saying who the suspect is." (Law enforcement DFI)*

- *"I can say that your model provides transparency in acquiring produced result for each given process." (Legal practitioner, Judge)*

- *"Because of its level of details, your model will facilitate collecting high quality evidence in a fast manner." (Law enforcement DFI)*

5.9.2 Usability

The 'usability' component of the Evaluation activity was intended to determine the ease with which experts in the law enforcement, commerce, incident response and legal domains can employ the CDFIPM to carry out those activities of the model that relate to

their practice. In response to the question of usability (see the questionnaire in section 5.6), "Please rate the model on the scale of 1 to 10, with 1 being very difficult to use and 10 being very easy to use.", experts provided the mean score of '8.7'. This also indicates that the CDFIPM has achieved its intended component of usability required of a useful artefact. The followings are some comments made by the experts in relation to the usability of the CDFIPM:

- *"This model is clear in its layout and the majority of its terms, which largely enables the user to understand the steps taken during the investigation without assistance. Where some of the terms are unclear or technical, the assistance of the explanation of a digital forensic investigator would overcome any difficulty in comprehension." (Legal practitioner, barrister)*

- *"It is important to have robust process behind the presentation of digital evidence because you have an adversarial system. Each seeks to undermine the evidence of the other if they can. Your model presents the forensic process very clearly; it is readily understandable to someone without technical expertise especially for jury." (Legal practitioner, judge)*

- *"Your model has a very clear layout that covers all aspects succinctly." (Law enforcement DFI)*

- *"I like the workflows as they are simple but effective." (Law enforcement DFI)*

5.10 Alterations Made to the CDFIPM

This section presents the modifications that were made to the abstract representation as well as the UML Activity Diagrams of the CDFIPM in response to the feedback provided by experts in section 5.8.2. Where a modification has been made, this is shaded and provided with its corresponding reference (addition, alteration or deletion) from the feedback in section 5.8.2.

5.10.1 Alterations to the CDFIPM's Abstract Representation

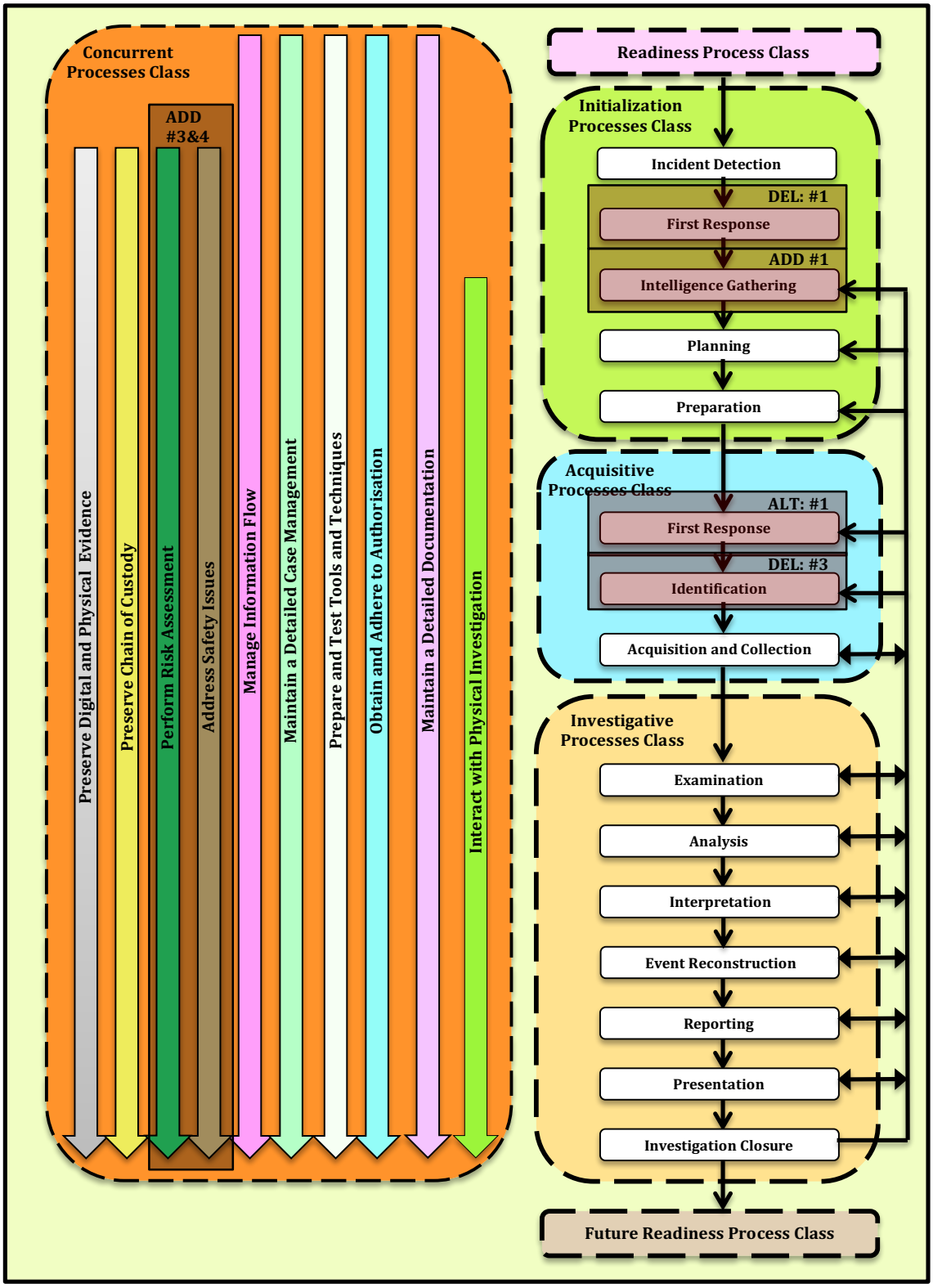


Figure 42. The modified version of the abstract representation of the CDFIPM

5.10.2 Alterations to the CDFIPM's Activity Diagrams

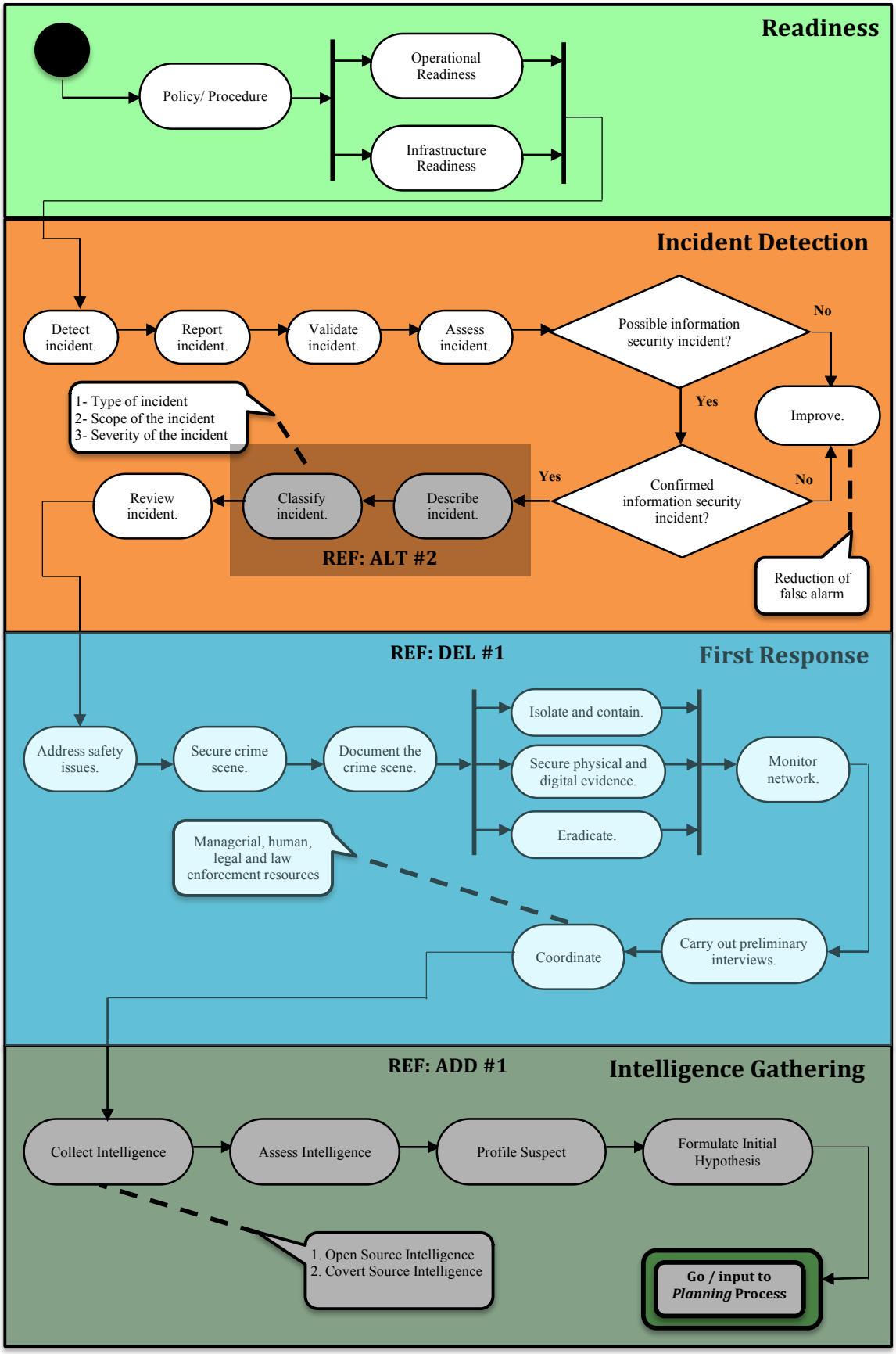


Figure 43. Amendment to the CDFIPM for ALT #2, DEL #1 and ADD #1

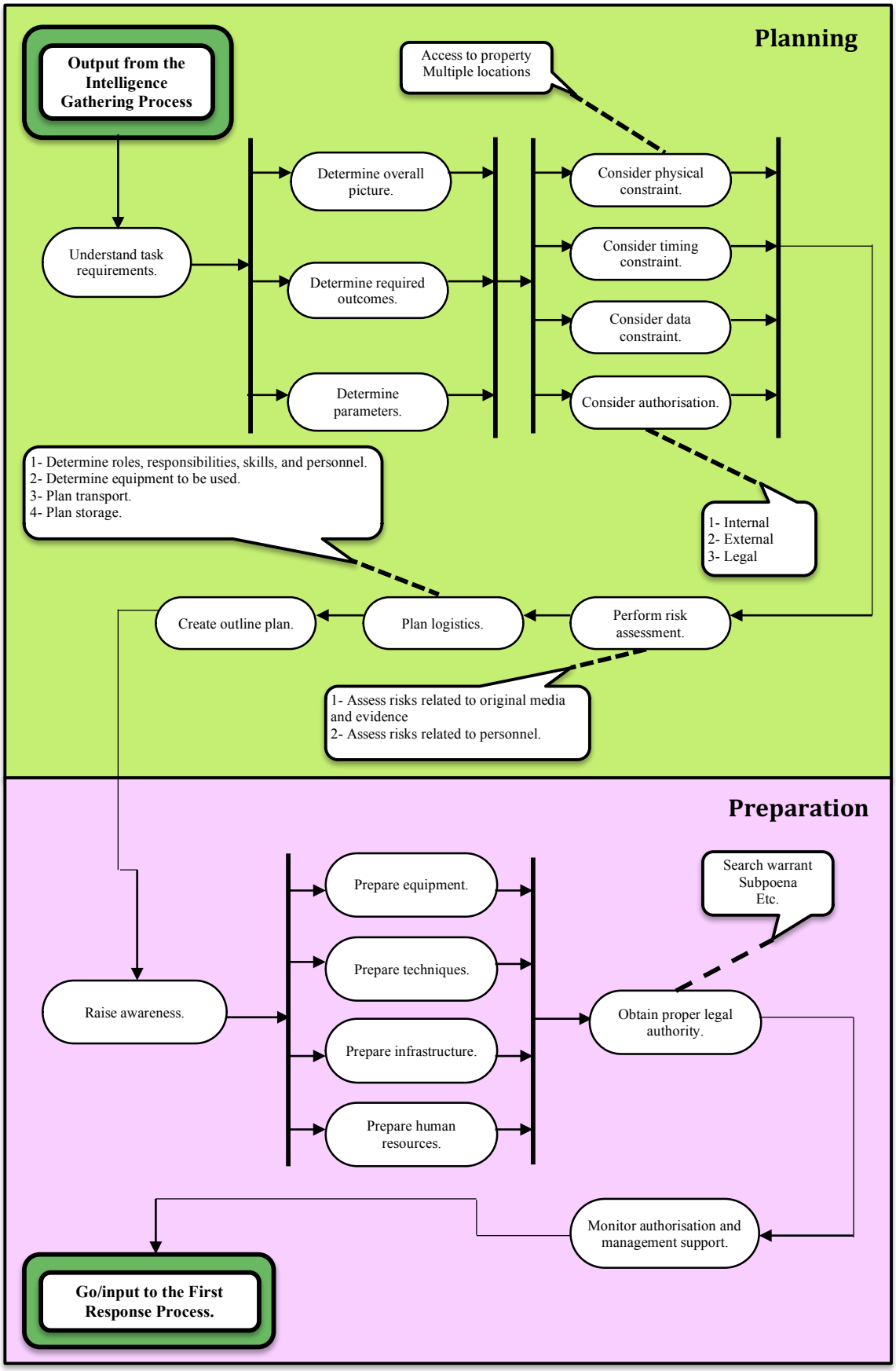


Figure 44. The CDFIPM's Planning and Preparation Processes, no amendment required

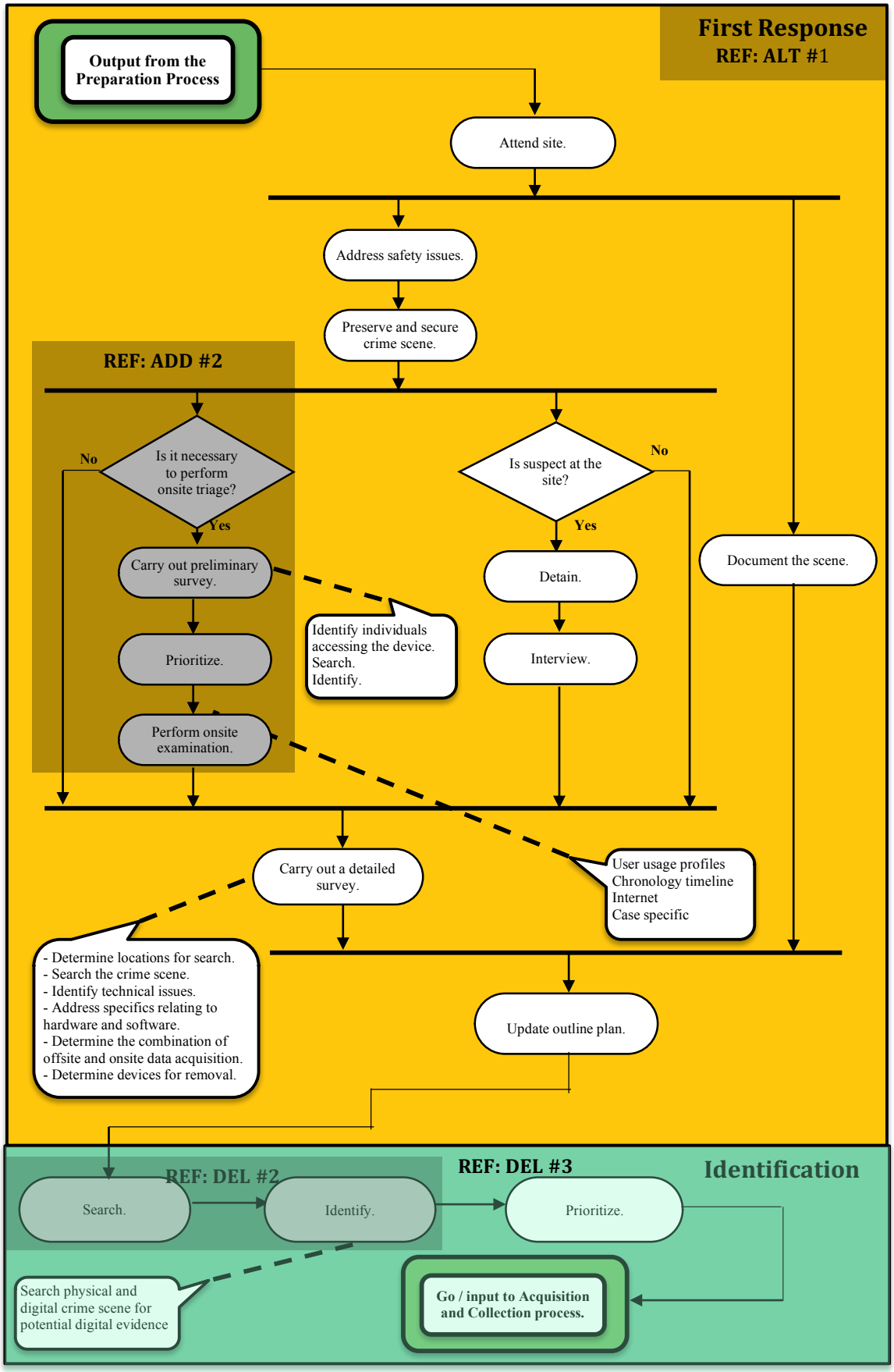


Figure 45. Amendment to the CDFIPM for ALT #1, ADD #2 and DEL #2 & #3

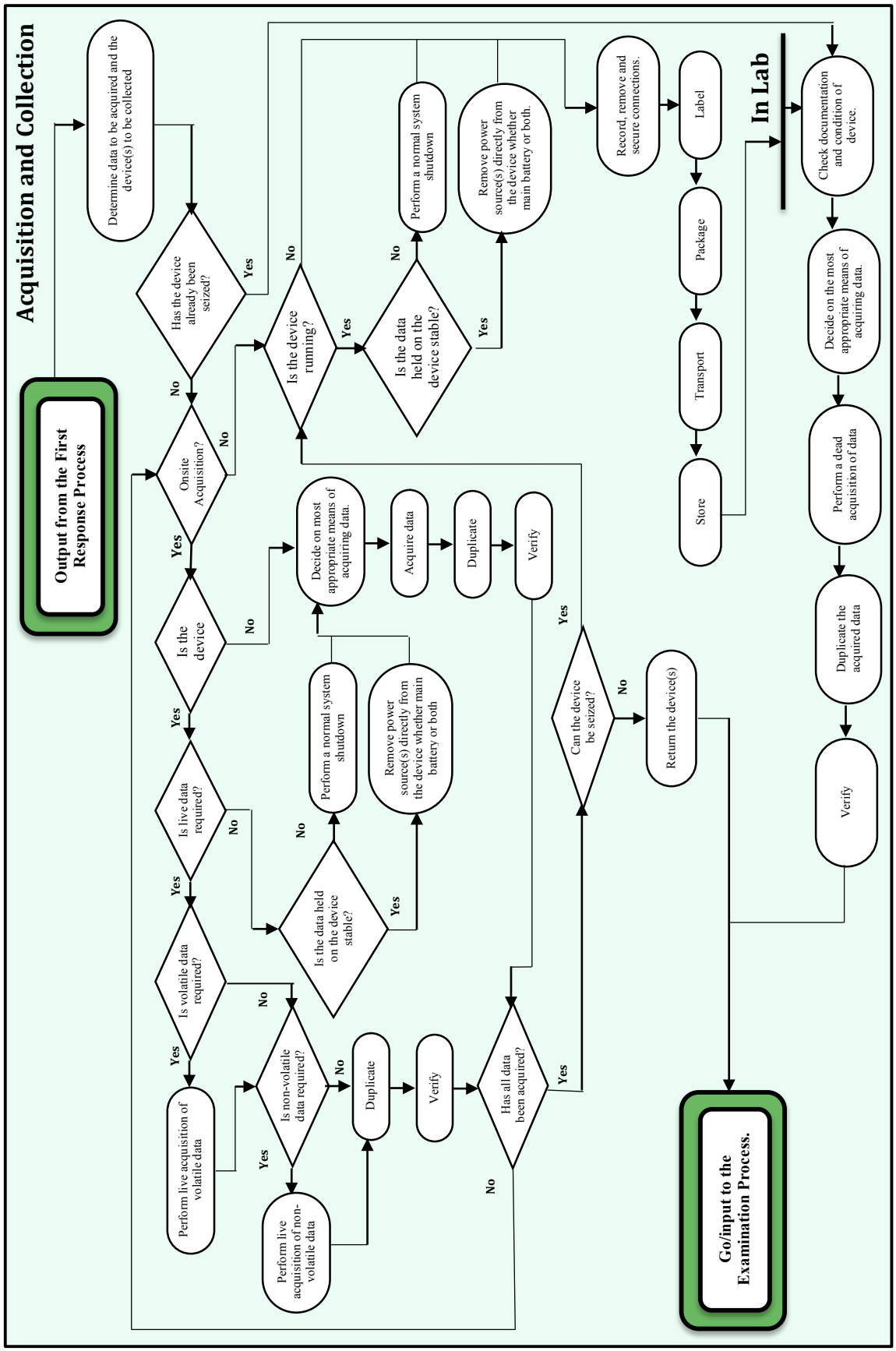


Figure 46. The CDFIPM's Acquisition and Collection Process, no amendment required

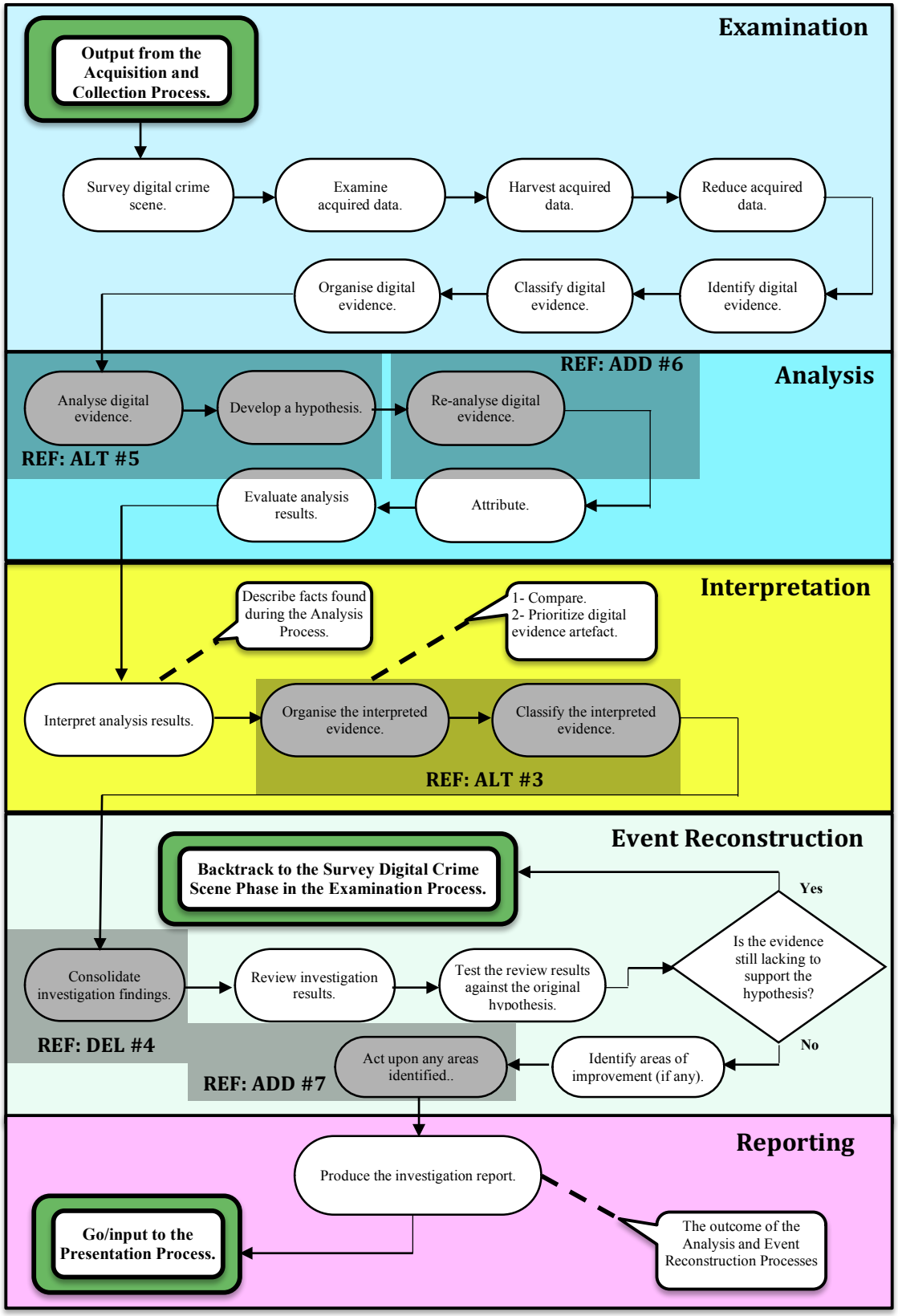


Figure 47. Amendment to the CDFIPM for ADD #6 & #7, ALT #3 & #5 and DEL #4

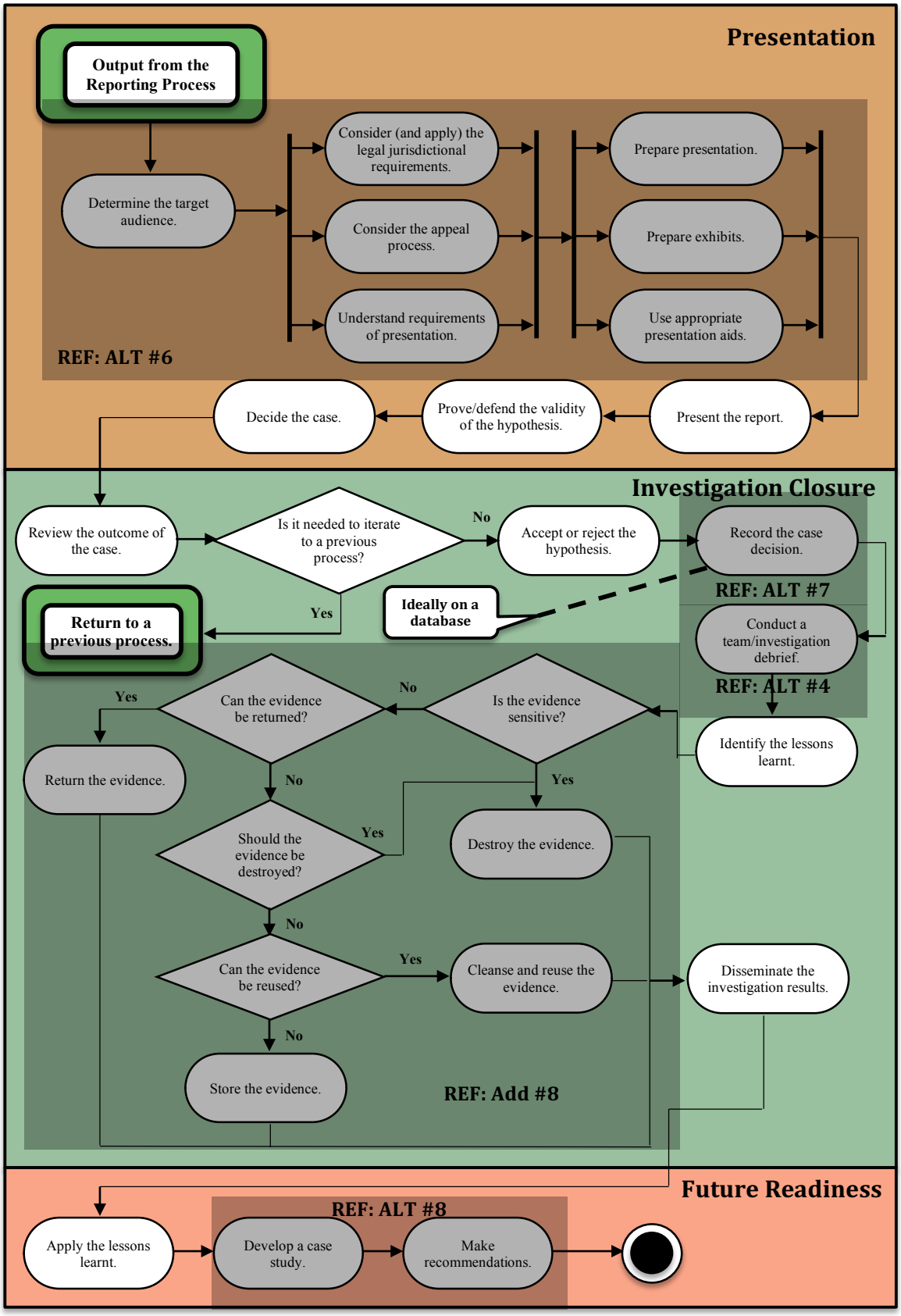


Figure 48. Amendment to the CDFIPM for ALT #4, #6, #7 & #8 and ADD #8

5.11 Final Version of the Proposed Model

The final versions of the abstract representation and the UML Activity Diagrams of the CDFIPM are presented in the Appendix B.

5.12 Assessing the CDFIPM against the Three Criteria

This section describes the process thorough which the proposed model was further evaluated by subjecting it to the same three sets of assessment criteria that the previously proposed models were subjected to in Chapter 2. This was to demonstrate how the CDFIPM itself would compare against the requirements outlined in those criteria, and also to judge the model even further.

5.12.1 Beebe and Clark Assessment Criteria

Just to recall the Beebe and Clark's (2005) four-point requirement, these are summarised as follows:

1. A model must achieve scientific rigor and relevance;
2. A model must simplify complex process to facilitate understanding of the underlying structure;
3. A model must retain enough granularity, or the flexibility to incorporate granularity needed to exploit the framework in unique situations; and
4. A model must delineate standard assumptions, concepts, value and practices.

It is contended that the CDFIPM has achieved all the criteria as outlined in the Beebe and Clark's (2005) four-point requirement. The followings justify such a claim:

Concerning Requirement 1, the CDFIPM has achieved both rigor and relevance since it is comprehensive such that it contains not only the higher-order layers, i.e. Classes and Processes, but also lower-level components, i.e. Phases and Sub-Phases, as well as important Overriding Principles. Rigor has been achieved through the use of a Phase approach and the inclusion of important Overriding Principles, while relevance has been

achieved through the use of objectives-based Sub-Phases. In terms of Requirement 2, the hierarchical nature of the CDFIPM allows complex process simplification by allowing its intended user community to focus on higher order layers conceptually. The CDFIPM has initially provided a simplified representation and abstract understanding of the overall investigative process at its highest level, i.e. Classes and Processes. This was to simplify the complex investigative process to facilitate understanding of the underlying structure. In relation to Requirement 3, the CDFIPM has then progressed to incorporate multiple layers of detail, i.e., Phases and Sub-Phases, to facilitate granularity. This, in turn, has achieved practicality and specificity goals set by its intended user community, digital forensic investigators, experts, legal practitioners and researchers alike. Finally, in terms of Requirement 4, the CDFIPM has delineated standard assumptions, concepts, values, and practices through the use of constraints, definitions, principles, objectives, and task hierarchies.

This argument that the CDFIPM has achieved all the four-point requirement set by Beebe and Clark (2005) is further confirmed by the positive feedback acquired from its intended user community discussed previously in this chapter.

5.12.2 Carrier and Spafford Assessment Criteria

The Carrier and Spafford's (2003) five-point requirement by which the proposed model can be further assessed are summarized as follows:

1. A model must have a basis in existing physical crime scene investigatory theory;
2. The model must be practical in that it matches the steps taken in actual investigations;
3. The model must be technologically neutral to ensure that the process isn't constrained by current products and procedures;
4. The model must have specificity to facilitate technology requirement development;
5. The model must be applicable to all possible user communities.

As with achieving all of the Beebe and Clark's (2005) criteria, the CDFIPM has also fulfilled all the criteria in the Carrier and Spafford's (2003) five-point requirement.

In relation to Requirement 1, the CDFIPM has clearly demonstrated that it has basis in the existing physical crime scene theory due to its implementation of the activities and Principles associated with physical investigation. An example of this relates to the components provided in the First Response Process, or the Overriding Principles such as Address Safety Issues or Perform Risk Assessment. Regarding Requirement 2, due to its level of detail demonstrated through its hierarchical approach, the CDFIPM has achieved the required level of practicality and specificity. Beebe and Clark state, "A framework that can handle the infusion of layers of detail will ultimately guide the practitioner regarding 'how to' and 'where to' find digital evidence (Beebe and Clark, 2005)." The CDFIPM can easily guide DFIs in any investigation due to its scientific approach demonstrated in model's granularity. The model has been applied to various case studies, and walkthroughs of the model have been performed. The model has also been tested by its various intended user communities. In relation to Requirement 3, the CDFIPM is also technologically neutral as it is not limited to a particular tool or technology. A concerted effort was made to apply scientific principles into the design and development of the CDFIPM to ensure such a neutrality. In terms of Requirement 4, the CDFIPM is detailed such that it can be used to aid the development and application of methodologies to new technologies as they emerge and become the subject of investigations. The CDFIPM has identified opportunities for development and deployment of technology to assist the work of DFIs. Finally, in relation to Requirement 5, the CDFIPM is generic in that it can be deployed across various fields of digital forensics.

5.12.3 Daubert Test Assessment Criteria

The Daubert Test's five-point requirement, against which the CDFIPM can be further assessed are summarized as follows:

1. whether the theory or technique in question can be and has been tested;
2. whether it has been subjected to peer review and publication;
3. its known or potential error rate;
4. the existence and maintenance of standards controlling its operation; and
5. whether it has attracted widespread acceptance within the relevant scientific community.

The CDFIPM has achieved the first four requirements as outlined in the Daubert Test. The model has been tested by its intended user community (Requirement 1), and as a result, its potential error rate was identified and subsequently rectified (Requirement 3). The model has also been subjected to peer-review and extensive publications in reputable journals and conferences, discussed in section 5.2 (Requirement 2). Furthermore, the CDFIPM's operation is governed by various existing standards and guidelines that the model has drawn upon such as ISO/IEC 27035, 27037, 27043 and ACPO Good Guide for Digital Evidence, etc. (Requirement 4). In terms of Requirement 5, this cannot be known at this point in time (as of June 2016) whether or not the model has been widely accepted by the digital forensic community. This will be determined over a few months or possibly years once the model is widely available to the digital forensic community. However, due to its detailed and scientific approach as well as the positive feedback that the model has received from its intended user community, it is anticipated that the CDFIPM will attract widespread acceptance within the field of digital forensics.

5.13 Comparison of the CDFIPM against Previous Models

The proposed model has also been mapped to the previously proposed models in Table 3 in order to reveal how the CDFIPM compares with these models. This comparison clearly demonstrates the comprehensiveness of the new model, as compared to the previous models. Those components of the CDFIPM that have matching components in the previous models will be marked using a "✔" sign over a grey cell background under the relevant previous model. Also, contributions of the CDFIPM in terms of new components will be highlighted in 'yellow' colour.

Table 3. Mapping the previous models to the proposed model

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
1. FRP	**1.1 Readiness**				✔	✔		✔	✔				✔							✔	
	1.1.1 Policy/ Procedure										✔		✔							✔	
	1.1.2 Operational Readiness				✔			✔					✔							✔	
	1.1.3 Infrastructure Readiness				✔			✔					✔							✔	
2. Initialization Processes Class	**2.1 Incident Detection**			✔	✔	✔	✔						✔						✔	✔	
	2.1.1 Detect Incident.			✔	✔	✔	✔						✔						✔	✔	
	2.1.2 Report Incident.				✔	✔	✔		✔		✔				✔					✔	
	2.1.3 Validate Incident.																				
	2.1.4 Assess Incident.								✔					✔						✔	
	2.1.5 Possible Information Security Incident																				
	2.1.6 Improve (Reduction of False Alarm).																				
	2.1.7 Confirm Incident.				✔	✔		✔						✔	✔					✔	
	2.1.8 Describe Incident.																				
	2.1.9 Classify Incident.																				
	2.1.9.1 Determine Type of Incident.																				
	2.1.9.2 Determine Scope of Incident.																				
	2.1.9.3 Determine Severity of Incident.																				
	2.1.10 Review Incident.																				
	2.2 Intelligence Gathering																				
	2.2.1 Collect Intelligence.																				
	2.2.1.1 Collect Open Source Intelligence.																				

To Be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
2. Initialization Processes Class	2.2.1.2 Collect Covert Source Intelligence.																				
	2.2.2 Assess Intelligence.																				
	2.2.3 Profile Suspect.																				
	2.2.4 Formulate Initial Hypothesis.																				
	2.3 Planning			✔			✔		✔		✔	✔	✔	✔	✔			✔	✔	✔	✔
	2.3.1 Understand Task Requirements.																				✔
	2.3.2 Determine Overall Picture.																				✔
	2.3.3 Determine Required Outcomes.																				✔
	2.3.4 Determine Parameters.																				✔
	2.3.5 Consider Timing Constraint.																				✔
	2.3.6 Consider Physical Constraint.																				✔
	2.3.6.1 Consider Access to Property.																				✔
	2.3.6.2 Consider Access to Multiple Locations.																				✔
	2.3.7 Consider Data Constraint.																				✔
	2.3.8 Consider Authorisation						✔														✔
	2.3.8.1 Internal, External or Legal						✔														✔
	2.3.9 Perform Risk Assessment																				
	2.3.9.1 Assess Risks Related to Original Media and Evidence.																				
	2.3.9.2 Assess Risks Related to Personnel.																				
	2.3.10 Plan Logistics.																				✔
	2.3.10.1 Determine Roles, Responsibilities, Skills, and Personnel.													✔							✔
	2.3.10.2 Determine Equipment To Be Used.																				
	2.3.10.3 Plan Transport.																				✔
	2.3.10.4 Plan Storage.																				✔

To Be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
2. Initialization Processes Class	2.3.11 Create Outline Plan																	✔			✔
	2.4 Preparation			✔					✔		✔							✔	✔		
	2.4.1 Raise Awareness.																				
	2.4.2 Prepare Equipment.																				
	2.4.3 Prepare Techniques.																				
	2.4.4 Prepare Infrastructure.																				
	2.4.5 Prepare Human Resources.																				
	2.4.6 Obtain Proper Legal Authority				✔	✔	✔	✔			✔		✔	✔	✔			✔	✔	✔	✔
	2.4.6.1 Search Warrant and Subpoena																				
	2.4.7 Monitor Authorisation and Management Support.																				
3. Acquisitive Processes Class	**3.1 First Response**				✔			✔	✔	✔			✔						✔		
	3.1.1 Attend Site.											✔						✔			✔
	3.1.2 Document the Crime Scene.				✔		✔		✔									✔	✔		✔
	3.1.3 Address Safety Issues.																	✔			✔
	3.1.4 Preserve and Secure Crime Scene.	✔		✔	✔	✔		✔	✔							✔	✔	✔		✔	
	3.1.5 Perform Onsite Triage If Necessary.											✔									
	3.1.6 Carry out Preliminary Survey.																				✔
	3.1.6.1 Identify Individuals Accessing the Device.																				
	3.1.6.2 Search.				✔	✔	✔	✔	✔		✔							✔		✔	
	3.1.6.3 Identify.	✔			✔		✔		✔	✔	✔					✔		✔	✔		
	3.1.7 Prioritize.																				
	3.1.8 Perform Onsite Examination.											✔									
	3.1.8.1 Examine User Usage Profiles.											✔									
	3.1.8.2 Examine Chronology Timeline.											✔									

To Be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
3. Acquisitive Processes Class	3.1.8.3 Examine Internet Browsing Activities.									✔		✔									
	3.1.8.4 Examine Case Specifics.											✔									
	3.1.9 Detain the Suspect If He Is at the Crime Scene.				✔							✔						✔			
	3.1.10 Interview the Suspect If He Is at the Crime Scene.																				
	3.1.11 Carry out A Detailed Survey.																				
	3.1.11.1 Determine Locations for Search																				
	3.1.11.2 Search the Crime Scene.				✔	✔	✔	✔	✔		✔							✔		✔	
	3.1.11.3 Identify Technical Issues.																				
	3.1.11.4 Address Specifics Relating to Hardware and Software.																				
	3.1.11.5 Determine Mix of Onsite and Offsite Data Acquisition.																				
	3.1.11.6 Determine the Devices for Removal.																				
	3.1.12 Update Outline Plan.																	✔			✔
	3.2 Acquisition and Collection	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	✔
	3.2.1 Determine Data and Device To Be Collected.																				
	3.2.2 Determine If the Device Has Already Been Seized.																				
	3.2.3 Determine If Onsite Acquisition Is Required.																				
	3.2.4 Determine If the Device Is Running.																				
	3.2.5 Determine If Live Data Is Required.																				
	3.2.6 Determine If Volatile Data Is Required.																				
	3.2.7 Determine If Non-Volatile Data Is Required.																				
	3.2.8 Perform Onsite Acquisition on a Powered-up Device.																				
	3.2.9 Perform Live Acquisition of Volatile Data.									✔			✔					✔			
	3.2.10 Preform Live Acquisition of Non-Volatile Data.									✔			✔								
	3.2.11 Perform Onsite Acquisition of a Powered-off Device.																				

To Be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
3. Acquisitive Processes Class	3.2.12 Determine If the Data Held on the Device Is Stable.																				
	3.2.13 Perform a Normal System Shut Down.																				
	3.2.14 Remove Power Source Directly from the Device.																				
	3.2.15 Decide on the Most Appropriate Means of Acquiring Data.																				✔
	3.2.16 Acquire Data.	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	✔
	3.2.17 Duplicate Data.																				
	3.2.18 Verify Data.																			✔	
	3.2.19 Determine If All Data Has Been Acquired.																				✔
	3.2.20 Determine If the Device Can Be Seized.																				
	3.2.21 Seize the Device.								✔											✔	✔
	3.2.22 Return the Device.			✔					✔					✔							✔
	3.2.23 Record, Remove and Secure Connections.																				
	3.2.24 Label.																				
	3.2.25 Package.																	✔			✔
	3.2.26 Transport.						✔				✔					✔		✔	✔	✔	✔
	3.2.27 Store						✔				✔					✔		✔	✔	✔	✔
	3.2.28 Check Documentation and Condition of the Device.																				✔
	3.2.29 Perform Offsite (Dead) Acquisition.	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	✔
	4.1 Examination	✔		✔	✔		✔		✔	✔	✔			✔		✔		✔		✔	
	4.1.1 Survey Digital Crime Scene.				✔				✔												
	4.1.2 Examine Acquired Data.	✔		✔			✔		✔	✔	✔			✔		✔		✔		✔	
	4.1.3 Harvest Acquired Data.								✔				✔							✔	
	4.1.4 Reduce Acquired Data.								✔				✔							✔	
	4.1.5 Identify Digital Evidence.																			✔	

To Be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
4. Investigative Processes Class	4.1.6 Classify Digital Evidence.																			✔	
	4.1.7 Organise Digital Evidence.												✔							✔	
	4.2 Analysis	✔		✔	✔				✔	✔	✔			✔		✔	✔	✔	✔	✔	
	4.2.1 Analyse Digital Evidence.	✔		✔	✔				✔	✔	✔			✔		✔	✔	✔	✔	✔	
	4.2.2 Develop a Hypothesis.						✔													✔	
	4.2.3 Re-Analyse Digital Evidence.																				
	4.2.4 Attribute.															✔				✔	
	4.2.5 Evaluate Analysis Results.																			✔	
	4.3 Interpretation															✔				✔	
	4.3.1 Interpret Analysis Results .															✔				✔	
	4.3.1.1 Describe Facts Found during the Analysis Process.																				
	4.3.2 Organise the Interpreted Evidence.																				
	4.3.2.1 Compare.																				
	4.3.2.2 Prioritize Digital Evidence Artefact.																				
	4.3.3 Classify the Interpreted Evidence.																				
	4.4 Event Reconstruction				✔	✔		✔	✔				✔			✔				✔	
	4.4.1 Review Investigation Results.																				
	4.4.2 Test the Review Results against the Original Hypothesis.																				
	4.4.3 Return to Examination Process If Evidence Is Still Lacking.																				
	4.4.4 Identify Areas of Improvement (If any).																				
	4.4.5 Act upon Any Areas Identified.																				
	4.5 Reporting		✔		✔				✔	✔			✔		✔			✔			
	4.5.1 Produce Investigation Report.		✔		✔				✔	✔			✔		✔			✔			
	4.5.1.1 Based on the Analysis and Event Reconstruction Processes																				

To Be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
4. Investigative Processes Class	**4.6 Presentation**	✔		✔	✔	✔	✔	✔	✔		✔			✔		✔	✔	✔	✔	✔	
	4.6.1 Determine the Target Audience.																				
	4.6.2 Consider and apply the Legal Jurisdictional Requirements.																				
	4.6.3 Consider the Appeal Process.																				
	4.6.4 Understand Requirements of the Presentation.																				
	4.6.5 Prepare Presentation.																				
	4.6.6 Prepare Exhibits.																				
	4.6.7 Use Appropriate Presentation Aids.																				
	4.6.8 Present the Report.																				
	4.6.9 Prove/ Defend the Validity of the Hypothesis.						✔		✔		✔										
	4.6.10 Decide the Case.	✔							✔											✔	
	4.7 Investigation Closure								✔												
	4.7.1 Review the Outcome of the Case.				✔	✔		✔	✔									✔		✔	
	4.7.2 Iterate to a Previous Process If Needed.																				
	4.7.3 Accept or Reject the Hypothesis.																				
	4.7.4 Record The Case Decision.																				
	4.7.5 Conduct a Team / Investigation Debrief.																				
	4.7.6 Identify the Lessons Learnt.																				
	4.7.7 Determine If the Evidence Is Sensitive.																				
	4.7.8 Destroy the Evidence.																				
	4.7.9 Determine If the Evidence Can Be Returned If Not Sensitive.																				
	4.7.10 Return the Evidence.			✔					✔					✔							✔
	4.7.11 Determine If the Evidence Should Be Destroyed.																				
	4.7.12 Determine If the Evidence Can Be Reused.																				

To be Continued …

Mapping the Existing DFIPMs to the Proposed Model (the CDFIPM)

The Proposed Model (CDFIPM)		Existing DFIPMs																			
		Palmer (2001)	Ashcroft (2001)	Reith et al. (2002)	Carrier and Spafford (2003)	Baryamureeba and Tushabe (2004)	Ciardhuáin (2004)	Rogers (2004)	Beebe and Clark (2005)	Kent et al. (2006)	Kohn et al. (2006)	Rogers et al. (2006)	Freiling and Schwittay (2007)	Khatir et al. (2008)	Selamat et al. (2008)	Cohen (2009)	Yusoff et al. (2011)	Agarwal et al. (2011)	Valjarevic and Venter (2012)	Kohn et al. (2013)	Adams et al. (2014)
	4.7.13 Cleanse and Reuse the Evidence.																				
	4.7.14 Store the Evidence.						✔				✔					✔		✔	✔	✔	✔
	4.7.15 Disseminate the Investigation Results.						✔		✔											✔	
5. FRPC	**5.1 Future Readiness**																				
	5.1.1 Apply the Lessons Learnt.																				
	5.1.2 Develop a Case Study.																				
	5.1.3 Make Recommendations.																				
6. Concurrent Processes Class	**6.1 Overriding Principles**								✔												✔
	6.1.1 Preserve Digital and Physical Evidence.						✔		✔										✔		
	6.1.2 Preserve Chain of Custody.						✔	✔					✔								✔
	6.1.3 Perform Risk Assessment.																				
	6.1.4 Address Safety Issues.																				
	6.1.5 Manage Information Flow.						✔		✔										✔		
	6.1.6 Maintain a Detailed Case Management.						✔		✔					✔							
	6.1.7 Prepare and Test Tools and Techniques.																				
	6.1.8 Obtain and Adhere to Authorisation.																				
	6.1.9 Maintain a Detailed Documentation.				✔	✔	✔	✔	✔					✔					✔	✔	
	6.1.10 Interact with Physical Investigation.				✔	✔		✔											✔	✔	

End of the Table

5.14 Summary of the Chapter

The CDFIPM has now been through a process of critical review and feedback by the leading experts in its intended user community, and subsequent process of alteration including new additions, amendments and deletions. This was to address the two components of 'utility' and 'usability' further by finding the answers to the two remaining questions ("has the model been built right?" and "has the right model been built?"). All the acquired feedback was very positive and there was no negative comment. In places where the agreement was not acquired, the thesis author iterated back to the Design and Development Phase of the research to make alterations based on the feedback to bring the model to the closest place possible (within the scope of the research) to its intended application. Having completed the formal evaluation of the CDFIPM, it is now contended that "the new model has been built right" and that "the right model has been built" on the basis that its intended application has been observed, accepted and confirmed by the prominent experts in its intended user community. Therefore, the CDFIPM is complete, consistent, and accurate enough to fulfill the solution to the stated research problem, as defined in section 1.2.

The proposed model was also assessed against the three sets of assessment criteria that the previously proposed models had been judged against in Chapter 2. The outcome of this assessment also revealed that the CDFIPM meets all the requirements as outlined in those criteria. The CDFIPM was finally mapped to the previous models demonstrating its comprehensiveness as compared to the previous models. Therefore, since the CDFIPM meets all the requirements levied upon it, this warrants the continuation of the steps as outlined in the Peffers et al's (2006) Design Science Research Process (DSRP), where the next step is to address the Communication activity of this research, which will be discussed in the next chapter, Conclusion.

Chapter 6: Conclusions

6.1 Introduction

This chapter begins by addressing the final activity of the Peffers et al's (2006) DSRP, namely Communication, before explaining how this research has accomplished the development of the CDFIPM (the research artefact) and extending the discussion to the question of how the CDFIPM could be employed in its intended user community. The research limitations are considered, as well as possible future research opportunities in the field of digital forensics. As previously, the chapter concludes with a short summary.

6.2 Communication

According to the Communication activity of the Peffers et al's (2006) DSRP, the researcher needs to communicate the research problem and its importance, the research artefact, its utility, usability and novelty, the rigor of its design, and its effectiveness to the intended user community. The first communication activity in relation to this research was conducted in 2015, when the CDFIPM in its very initial stage was presented both orally and as a research paper at the 10th International Conference on Global Security, Safety & Sustainability, held in London. The summit was attended by both national and international renowned participants from law enforcement, industry and academia, who provided brief but valuable comments on the initial stage of the CDFIPM. Following the formal evaluation of the CDFIPM by its intended user community[39], a Deputy High Court Judge based in Exchange Chambers in Manchester, Leeds and Liverpool who is the current Chairman of the Northern Chancery Bar Association (as of May 2016) and is a Trustee of the North West Partnership, has expressed interest in employing the CDFIPM when dealing with cases involving computer crimes.

[39] These include: digital forensic investigators operating in three fields of law enforcement, commercial practice and incident response, judges, legal practitioners, those in the research community in the fields of digital forensics and information security and other relevant audiences.

Extracts from this research and the CDFIPM have also been published or accepted for publications in the following peer-reviewed journals and conference proceedings:

- Montasari, R (2016). 'An Ad Hoc Detailed Review of Digital Forensic Investigation Process Models', *International Journal of Electronic Security and Digital Forensics (IJESDF),* 8 (3), pp. 205-223.

- Montasari, R (2016). 'A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensics Practice', *International Journal of Computer Science and Security (IJCSS),* 10 (2), pp. 69-87.

- Montasari, R. (2016). 'A Comprehensive Digital Forensic Investigation Process Model', *International Journal of Electronic Security and Digital Forensics (IJESDF),* 8 (4), pp. 285-301.

- Montasari, R. (2016). 'Review and Assessment of the Existing Digital Forensic Investigation Process Models', *International Journal of Computer Applications,* 147 (7), pp. 41-49.

- Montasari, R., Peltola, P. and Carpenter, V. (2016). 'Gauging the Effectiveness of Computer Misuse Act in Dealing with Cybercrimes', *International Conference on Cyber Security and Protection of Digital Services,* pp. 1-5.

- Montasari, R., Peltola, P. and Evans, D. (2015). 'Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 83-95.

- Montasari, R. and Peltola, P. (2015). 'Computer Forensic Analysis of Private Browsing Modes', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 96-109.

- Montasari, R. (in press). 'Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction', *Proceedings of 11th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*.

- Montasari, R. (in press). 'A Standardized Data Acquisition Process Model (SDAPM) for Digital Forensic Investigations', *International Journal of Information and Computer Security (IJICS)*.

6.3 Research Summary

In **Chapter 1**, three major issues were identified with the existing digital forensic investigation process models (DFIPMs), namely the lack of a model that has all three characteristics of being "comprehensive", "formal" and "generic". The research therefore set out to address the fundamental problem that:

> *There does not exist a comprehensive model encompassing the entire digital investigative process that is formal, such that it can assist a court of law in determining the reliability of the investigative process followed, and that is generic, in that it can be applied in the different fields of law enforcement, commerce and incident response.*

Following the identification of the research problem, two research hypotheses were developed as follows:

> *A formal process model can be developed that is comprehensive in that it encompasses the whole digital forensic process and that is generic in that it can be employed by the digital forensic investigators in the fields of law enforcement, commerce and incident response.*

> *A formal process model will enable digital forensic investigators to carry out more effective, forensically-sound digital investigations than is possible with the use of ad-hoc tools, and will assist the courts in determining the reliability of the processes employed in such investigations.*

In order to address the research problem and prove or refute the research hypotheses, the following research aim was then formulated:

> *To develop a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonises and extends the existing models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response.*

In order to achieve the aim, the following objectives were set out to be accomplished:

1. Critically analyse and assess the previous DFIPMs against different assessment criteria in order to identify the models that can contribute to the design and development of the new model.

2. Following the identification of the prevailing models (those that have withstood the assessment), determine their key contributions based on the assessment criteria.

3. Identify the components essential for the new model from a combination of the key contributions of both the prevailing and the reviewed models.

4. Build upon the contributions of the previous models by constructing a new set of domain-specific components.

5. Based upon the above preceding steps, design and develop a formal representation of the new model, incorporating both the identified components and the new set of constructed components.

6. Evaluate the model using three methods, including applying the model to different case studies, assessing it against the different assessment criteria used to assess the previous models and recruiting different sets of independent experts.

To achieve those objectives, three research questions were sought to be answered:

1. What are the essential components necessary in a comprehensive model that is formal, generic and forensically sound for the entire digital forensic process?

2. Once the components of such a comprehensive model that is formal, generic and forensically sound are determined, how can they be integrated into a working model?

3. What is the most appropriate method to describe, present and use the model for the entire digital forensic process?

Finally, in Chapter 1, to answer the three research questions, the Peffers et al's (2006) Design Science Research Process (DSRP) model was identified and justified as the appropriate methodology to carry out the various stages of this research.

In **Chapter 2,** based upon the Peffers et al's (2006) DSRP, the acquisition of two resources was sought in order to define the "objectives of the solution". These included: "… knowledge of the state of the problem" and "current solutions and their efficacy, if any". The knowledge of the state of the problem for this research was partly covered in the preceding chapter (Chapter 1), where the research problem was defined and the value of its solution justified. However, to address the two resources fully, further knowledge of the state of the problem was required and current solutions, if any, had to be identified. In order to acquire the two stated resources, a general review of the topic of digital forensic investigation was provided, followed by a detailed review of the field of digital evidence and how its admissibility is governed within the U.K. and U.S. jurisdictions. Current standards and guidelines associated with the digital investigative process were then reviewed, which set the necessary background for a review and assessment of the previous models. Prior to such review and assessment, three different sets of assessment criteria were identified against which the previous models were reviewed and assessed. Through this assessment, the prevailing models that could contribute to the design and development of the CDFIPM were identified, and the necessary components that would constitute the basic structure of the new model were determined.

Chapter 3 covered the Design and Development activity of the Peffers et al's (2006) DSRP, implementing design and development of the CDFIPM based upon the information acquired in Chapter 2 in relation to the three research questions. After considering the fundamental requirements of the CDFIPM, there followed a detailed discussion of its design elements, where the CDFIPM's formal representation was examined and the use of UML Activity Diagrams was justified. Further examination was made in relation to the hierarchical structure of the CDFIPM before a detailed analysis of the design and development of the model was undertaken. The CDFIPM was also presented in its various layers of granularity through the use of the UML Activity Diagrams.

Chapter 4 covered the Demonstration activity of the Peffers et al's (2006) DSRP, applying the CDFIPM to various case scenarios representing different digital forensic environments, thereby demonstrating the efficacy of the proposed model to solve the stated research problem.

Finally, **Chapter 5** covered the Evaluation activity of the Peffers et al's (2006) DSRP, where the CDFIPM was subjected to external, independent evaluation by its intended user community to determine how well the new model would support a solution to the stated research problem. Following feedback from the experts, it was necessary to return to the Design and Development stage to make various amendments before presenting the CDFIPM in its amended form.

6.4 Research Questions Addressed

To achieve the research objectives, the following three research questions were sought to be answered:

1. What are the essential components necessary in a comprehensive model that is formal, generic and forensically sound for the entire digital forensic process?

2. Once the components of such a comprehensive model that is formal, generic and forensically sound are determined, how can they be integrated into a working model?

3. What is the most appropriate method to describe, present and use the model for the entire digital forensic process?

Question one has been answered by conducting a critical review and detailed assessment of the existing models in Chapter 2 using three different assessment criteria, namely those of Beebe and Clark (2005), Carrier and Spafford (2003) and the Daubert Test (*Daubert v. Merrell Dow Pharmaceuticals,* 1993). Following a review of the assessment results, the prevailing models (those that most closely met the assessment criteria) were identified for consideration of their potential contribution towards the new model. Having identified the prevailing models, their key contributions were determined based on the assessment criteria, and the necessary components for the CDFIPM were identified from these key contributions. The author was then able to develop a new set of domain-specific components, based upon the knowledge acquired through interactions with experts that could not be found in the literature.

Question two was addressed during the Design and Development stage of the research in Chapter 3, where the identified components and the developed domain-specific components were integrated into the CDFIPM through the use of the UML Activity Diagrams. Question three was addressed first in Chapter 4 and then in Chapter 5. In Chapter 4, case scenarios having been identified as the most appropriate method to use and describe the new model, the CDFIPM was applied to different scenarios and a walkthrough of the model was performed. Question three was then independently addressed by external experts, the model's intended user community, who evaluated the CDFIPM based upon the three elements of "rigor", "usability" and "utility" to determine its suitability for the environments[40] in which the CDFIPM is intended to be employed. To further demonstrate the suitability of the CDFIPM, a practical experimentation was conducted, presented in Appendix A.

[40] This includes: law enforcement, commerce and incident response, as well as court environments.

6.5 Research Objectives Achieved

In order to achieve the research aim, the following objectives needed to be accomplished:

1. Critically analyse and assess the previous DFIPMs against different assessment criteria in order to identify the models that can contribute to the design and development of the new model.

2. Following the identification of the prevailing models (those that have withstood the assessment), determine their key contributions based on the assessment criteria.

3. Identify the components essential for the new model from a combination of the key contributions of both the prevailing and the reviewed models.

4. Build upon the contributions of the previous models by constructing a new set of domain-specific components.

5. Based upon the above preceding steps, design and develop a formal representation of the new model, incorporating both the identified components and the new set of constructed components.

6. Evaluate the model using three methods, including applying the model to different case studies, assessing it against the different assessment criteria used to assess the previous models and recruiting different sets of independent experts.

The research objectives have been achieved by addressing the three research questions set out in section 6.4. The first four objectives were achieved in Chapter 2, where three assessment criteria were identified against which the previous models were assessed. This assessment identified those prevailing models that could contribute to the design and development of the CDFIPM. Following the identification of the prevailing models, their key contributions were determined, and the necessary components for the

CDFIPM were identified from these key contributions. A new set of domain-specific components were developed through the knowledge acquired from interaction with experts. Objective 5 was achieved in Chapter 3, the CDFIPM being designed and developed by synthesizing the components identified from the key contributions of the prevailing models with the new set of domain-specific components. Their integration was achieved into the CDFIPM through the use of UML Activity Diagrams. Finally, objective six was achieved in two stages, by applying the CDFIPM to different case scenarios and by performing a walkthrough of the model in Chapter 4 and by subjecting the model to an independent evaluation by its intended user community in Chapter 5.

6.6 Research Aim Achieved

In order to address the research problem and to prove or refute the research hypothesis, the following research aim was formulated:

> *To develop a comprehensive model encompassing the entire digital investigative process that is formal in that it synthesizes, harmonises and extends the existing models, and that is generic in that it can be applied in the different fields of law enforcement, commerce and incident response.*

The research aim has been accomplished as the objectives set out to achieve the research aim have been fulfilled (see section 6.5) by addressing the three research questions (see section 6.4). In summary, to develop the model in such a way that it could be both formal and generic to the three fields of law enforcement, commerce and incident response, the common components from the "prevailing" models across the three fields were identified, then synthesized, harmonised and extended (in Chapter 2) and subsequently integrated into a comprehensive model covering the entire investigative process (in Chapter 3). The final CDFIPM was represented through the use of formal notations, the UML Activity Diagrams.

6.7 Research Problem Addressed

In order to address the three identified issues with the existing models in relation to the lack of a model that has all the three characteristics of being "comprehensive", formal" and "generic", the following research problem was formulated that needed to be addressed:

> *There does not exist a comprehensive model encompassing the entire digital investigative process that is formal, such that it can assist a court of law in determining the reliability of the investigative process followed, and that is generic, in that it can be applied in the different fields of law enforcement, commerce and incident response.*

The research problem has also been addressed through the accomplishment of the research aim discussed in section 6.6. Therefore, having addressed the research problem, the two formulated research hypotheses also hold true:

> *A formal process model can be developed that is comprehensive in that it encompasses the whole digital forensic process and that is generic in that it can be employed by the digital forensic investigators in the fields of law enforcement, commerce and incident response.*

> *A formal process model will enable digital forensic investigators to carry out more effective, forensically-sound digital investigations than is possible with the use of ad-hoc tools, and will assist the courts in determining the reliability of the processes employed in such investigations.*

This is further supported by the external feedback acquired from the CDFIPM's intended user community (discussed in detail in Chapter 5).

6.8 Research Contribution

It is contended that this research has made a significant and novel contribution to the field of digital forensic science by implementing a process model, the CDFIPM, that would assist digital forensic investigators in following a uniform approach. The research has synthesized, harmonised and significantly built upon the existing models to produce the first process model that has all three characteristics of being comprehensive, formal and generic. No such a model previously existed in the literature.[41] The CDFIPM is comprehensive, covering the entire investigative process, formal as it assists courts in determining the reliability of the investigative process followed and generic in that it can be applied by digital forensic investigators operating in the three fields of law enforcement, commerce and incident response. The author maintains that the proposed model is inclusive of all the advantages of the previous models through their synthesis and harmonisation, and contains purified terminology using the terms commonly agreed upon by the digital forensic community.

It is therefore argued that the CDFIPM would be a significant step towards the establishment of standards for the digital forensic investigative process. Every component in the model is well defined in terms of scope, functions and order. The CDFIPM has exceeded the steps needed to acquire, preserve, examine and analyse digital evidence, also incorporating the non-technical aspects of a digital investigation, including authorization, notification, proof, defence and transportation of evidence. The model fully and thoroughly describes the flow of information in a digital investigation, from the moment digital investigators are notified of a crime until the investigation reaches its formal conclusion.

This research has also demonstrated how the entire digital investigative process, both in its high-level and lower-level details, can be represented through a proven formal notation, the Unified Modelling Language (UML). The representation of the CDFIPM via the UML Activity Diagrams will assist courts in properly understanding the digital investigative processes followed, a point acknowledged by the legal practitioners and judge who participated in an external evaluation of the model.

[41] Table 2 sets out the specific contributions of this research in relation to the CDFIPM's components, highlighted in "yellow".

Due to its level of details and step-by-step approach, the CDFIPM provides investigators with concise direction on the processes to be followed, enabling them to speed up the investigative process while minimising errors and negligence. Therefore, in the event of a challenge to the digital investigative process, there would be no doubt concerning the soundness of the processes followed. The proposed model also contains generic methods that digital forensic investigators can use to relate technology to non-technical observers. Importantly, the application of the CDFIPM could bring about the improved admissibility of digital evidence in courts, being a formal model with strong overriding principles resulting from rigorous scientific verification. Finally, this thesis contains the most comprehensive, critical review and assessment of the previous digital investigation process models presented to date.

6.9 Limitations and Future Work

Although the CDFIPM is mainly aimed at the U.K. jurisdiction, it could easily be adapted to other jurisdictions. Without such modification, the model already has relevance to those jurisdictions which employ a similar legal basis for evaluating the digital investigative process. The CDFIPM focuses predominantly on "Computer Forensics" as opposed to other branches of digital forensics.[42] Although some much simpler models have claimed to be appropriate for various branches of digital forensics, such a claim is not made in relation to the CDFIPM for accuracy purposes. However, it is argued that due to the CDFIPM's detailed and generic approach, it could easily be adapted to cover any branch of digital forensics. Although an evaluation of the CDFIPM has been undertaken by the High-Tech Crime Units (HTCUs) of two different police forces in the U.K., experts in corporate and incident response environments, legal practitioners and researchers in academia, it cannot be representative of all intended users. Future work should include a more comprehensive trial by digital forensic investigators, experts, legal practitioners and researchers as part of a wider study.

Similarly, although the case scenarios to which the CDFIPM was applied represent each of the three fields of digital forensics to which the model is relevant, the CDFIPM would benefit from further case studies to identify task hierarchies. This would

[42] Such as Malware Forensics, Cloud Forensics, Network Forensics and Mobile Forensics.

improve task development efforts and facilitate scenario development, assisting its users, researchers and tool developers in understanding how to take advantage of and apply the model. Finally, as with the future work, the CDFIPM must be validated through the Method Validation under ISO 17025 accreditation[43], which will be published in the U.K. within the next 18 months (as of June 2016), to determine its compliance.

6.10 Summary of the Chapter

This chapter has outlined the way in which this research has been communicated and has provided a summary of the research, describing how the research problem, hypothesis, aim, objectives and questions have been addressed, before analyzing the contributions of the research, its research limitations and the potential future research opportunities.

[43] The Forensic Science Regulators (2016) will require that all Forensic Service Providers providing a Digital Forensic Service have ISO 17025 Accreditation, which will soon become the UK's Best Practice Guidance.

References

AccessData. (2016). Forensic Toolkit (FTK). Available at: http://accessdata.com/products/computer-forensics/ftk (Accessed: 09 June 2016).

ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence*. U.K. Association of Chief Police Officers. Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 10 June 2016).

Adams, L. and Courtney, J. (2004). 'Achieving Relevance in IS Research via the DAGS Framework', *37th Hawaii International Conference on System Sciences*, pp. 1-10.

Adams, J., Khan, H., Raeside, R. and White, D (2007). *Research Methods for Graduate Business and Social Science Students*. 2nd edn. India: SAGE Publications.

Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice*. PhD thesis. Murdoch University.

Adams, R., Hobbs, V. and Mann, G. (2014). 'The advanced data acquisition model (ADAM): a process model for digital forensic practice', *Journal of Digital Forensics, Security and Law,* 8(4), pp.25–48.

Agarwal, A., Gupta, M., Gupta, S. and Gupta, C. (2011). 'Systematic digital forensic investigation model', *International Journal of Computer Science and Security,* 5(1), pp.118–130.

Aken, V. and Ernst, J. (2005). 'Management Research as a Design Science: Articulating the Research Products of Mode 2 Knowledge Production in Management', *British Journal of Management,* 16(1), pp.19-36.

Archer, L. (1984). *Systematic Method for Designers*. London: John Wiley.

Armstrong, S. (2006). 'Findings from evidence-based forecasting: Methods for reducing forecast error', *International Journal of Forecasting*, 22(3), pp. 583-598.

Armstrong, C. and Armstrong, H. (2010). 'Modeling Forensic Evidence Systems Using Design Science', *IFIP WG 8.2/8.6 International Working Conference*, pp.282-300.

Ashcroft, J. (2001). *Electronic Crime Scene Investigation: A Guide for First Responders*. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (Accessed: 10 June 2016).

Ashcroft, J., Daniels, D. and Hart, S (2004). *Forensic Examination of Digital Evidence: a Guide for Law Enforcement*. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Accessed: 10 June 2016).

Balci, O. (2004). 'Quality Assessment, Verification, and Validation of Modeling and Simulation Applications', *Proceedings of the 2004 Winter Simulation Conference*, pp. 1-8.

Baldwin, J. (1993). 'Police Interview Techniques Establishing Truth or Proof?', *British Journal of Criminology*, 33(3), pp.325–352.

Ball, C. (2008). 'What Judges Should Know About Computer Forensics', *National Workshop for District Judges II*, pp. 1-19.

Barlas, Y. (1996). 'Formal aspects of model validity and validation in system dynamics', *System Dynamics Review*, 12(3), pp. 183-210.

Baryamureeba, V. and Tushabe, F. (2004). 'The Enhanced Digital Investigation Process Model', *4th Digital Forensic Research Workshop*, pp. 1-9.

Beebe, N. and Clark, J. (2005). 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process', *Digital Investigation,* 2(2), pp.147–167.

Bem, D., Feld, F., Huebner, E. and Bem, O. (2008). 'Computer Forensics - Past, Present and Future', *Journal of Information Science and Technology,* 5(3), pp. 43–59.

Bernstein, D. (2008). 'Expert Witnesses, Adversarial Bias, and the (Partial) Failure of the Daubert Revolution', *George Mason University Law and Economics Research Paper*, 93(451), pp. 100-137.

Black, I. (2014). *The Art of Investigative Interviewing.* 3rd edn. Boston: Butterworth Heinemann.

Boddington, R., Hobbs, V. and Mann, G. (2008). 'Validating digital evidence for legal argument', *6th Australian Digital Forensics Conference*, pp. 1-16.

Bogen, C. and Dampier, D. (2005). 'Unifying Computer Forensics Modeling Approaches: A Software Engineering Perspective', *1st International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 27-39.

Booker, J. and McNamara, L. (2004). 'Solving black box computation problems using expert knowledge theory and methods', *Reliability Engineering & System Safety*, 85(1), pp. 331-340.

Boote, D. and Beile, P. (2005). 'Scholars Before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation', *Educational Researcher*, 34(6), pp. 3-15.

British Standards Institution. (2014). BS 10008:2014. *Evidential Weight and Legal Admissibility of Electronic Information*. London: British Standards Institution.

Brown, C. (2006). *Computer Evidence: Collection and Preservation.* Charles River Media.

Brown, C. (2009). *Computer Evidence: Collection and Preservation*. 2nd edn. Boston: Course Technology.

Bryman, A. (2015). *Social Research Methods.* 5th edn. Oxford: Oxford University Press.

Bulbul, H., Yavuzcan, H. and Ozel, M. (2013). 'Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM)', *Forensic Science International*, 233(1), pp.244-256.

Burgman, M., Carr, A., Godden, L., Gregory, R., McBride, M., Flander, L. and Maguire, L. (2011). 'Redefining expertise and improving ecological judgment', *Conservation Letters*, 4(2), pp. 81-87.

Burrell, G. and Morgan, G. (1985). *Sociological Paradigms and Organisational Analysis: Elements of the Sociology of Corporate Life*. Farnham: Ashgate Publishing Group.

Buskirk, E. and Liu, V. (2006). 'Digital Evidence: Challenging the Presumption of Reliability', *Journal of Digital Forensic Practice*, 1(1), pp. 19-26.

Calhoun, M. (2008). 'Scientific Evidence in Court: Daubert or Frye, 15 Years Later', *Legal Backgrounder,* 23(37), pp.1-4.

Carlton, H. and Worthley, R. (2009). 'An evaluation of agreement and conflict among computer forensic experts', *42nd Hawaii International Conference on System Sciences*, pp. 1-10.

Carrier, B. (2002). Open Source Digital Forensics Tools: The Legal Argument. Available at: http://www.cs.plu.edu/courses/netsec/arts/osf.pdf (Accessed: 28 June 2016).

Carrier, B. and Spafford, E. (2003). 'Getting Physical with the Digital Investigation Process', *International Journal of Digital Evidence*, 2(2), pp.1–20.

Carrier, B. and Spafford, E. (2004). 'An Event-Based Digital Forensic Investigation Framework', *4th Digital Forensic Research Workshop*, pp.1–12.

Carrier, B (2005). *File System Forensic Analysis*. Boston: Addison Wesley.

Casey, E. (2002). 'Error, Uncertainty, and Loss in Digital Evidence', *International Journal of Digital Evidence*, 1(2), pp. 1-45.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd edn. New York: Elsevier Academic Press.

Ciardhuáin, O. (2004). 'An Extended Model of Cybercrime Investigations', *International Journal of Digital Evidence*, 3(1), pp. 1-22.

Clemen, R. and Winkler, R. (1999). 'Combining Probability Distributions From Experts in Risk Analysis', *Risk Analysis*, 19(2). pp. 187-203.

Cohen, F. (2009). *Digital Forensic Evidence Examination*. 2nd edn. Livermore, California: Fred Cohen & Associates.

Cohen, F. (2010). 'Towards a Science of Digital Forensic Evidence Examination', *6th IFIP WG 11.9 International Conference on Digital Forensics*, pp. 17-35.

Cohen, F. (2011). 'Putting the Science in Digital Forensics', *Journal of Digital Forensics, Security and Law*, 6(1), pp.7–14.

Cohen, F., Lowrie, J. and Preston, C. (2011). 'The State of the Science of Digital Evidence Examination', *7th IFIP WG 11.9 International Conference on Digital Forensics*, pp. 3-21.

Cohen, F. (2012). 'Update on the State of the Science of Digital Evidence Examination', *Proceedings of the Conference on Digital Forensics, Security, and Law*, pp.7–18.

Cooke, R. (1991). *Experts in Uncertainty: Opinion and Subjective Probability in Science*. New York: Oxford University Press.

Cooke, R. and Goossens, L. (2000). 'Procedures Guide for Structural Expert Judgement in Accident Consequence Modelling', *Radiation Protection Dosimetry*, 90(3), pp. 303-309.

Cook, D. and Skinner, J. (2005). 'How to Perform Credible Verification, Validation, and Accreditation for Modeling and Simulation', *The Journal of Defense Software Engineering*, 18 (5), pp. 20-24.

Cornell University Law School. (2016). Daubert Standard. Available at: https://www.law.cornell.edu/wex/daubert_standard (Accessed: 21 June 2016).

Cowling, R. and Pressey, R. (2003). 'Introduction to systematic conservation planning in the Cape Floristic Region', *Biological Conservation,* 112(1), pp. 1-13.

Czembor, C. and Vesk, P. (2009). 'Incorporating between-expert uncertainty into state-and-transition simulation models for forest restoration', *Forest Ecology and Management*, 259(2), pp. 165-175.

Dattu, F. (1998). 'Illustrated jury instructions: A proposal', *Law and Psychology Review*, 22, pp. 67-102.

Design Science Journal. (2016). Welcome to Design Science Journal. Available at: http://www.designsciencejournal.org/ (Accessed: 28 June 2016).

Dictionary.com. (2016). Harmonise. Available at: http://www.dictionary.com/browse/harmonise?s=t (Accessed: 28 June 2016).

Drescher, M., Perera A., Buse L., Ride, K. and Vasiliauskas, S. (2008). 'Uncertainty in expert knowledge of forest succession: a case study from boreal Ontario', *The Forestry Chronicle,* 84(2), pp. 194-209.

Eddy, D., Hollingworth, W., Caro, J., Tsevat, J., McDonald, K. and Wong, J. (2012). 'Model Transparency and Validation A Report of the ISPOR-SMDM Modeling Good Research Practices Task Force–7', *Medical Decision Making*, 32(5), pp. 733-743.

Edirisuriya, A. (2009). *Design Support for e-Commerce Information Systems Using Goal, Business and Process Modelling*. PhD thesis. Stockholm University.

Eekels, J., and Roozenburg, N. (1991). 'A methodological comparison of the structures of scientific research and engineering design: their similarities and differences', *Design Studies*, 12(4), pp. 197-203.

Farmer, D., Venema, W. (2005). *Forensic Discovery*. Upper Saddle River: Addison-Wesley.

Farrell, M. (1993). Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemilogy and Legal Process. *Cardozo L. Rev.*, *15*, p. 2183.

Fisher, L. (2009). *The Perfect Swarm: The Science of Complexity in Everyday Life*. New York: Basic Books.

Ford, D. and Sterman, J. (1998). 'Expert knowledge elicitation to improve formal and mental models', *System Dynamics Review*, 14(4), pp.309-340.

Forensic Science Regulator. (2016). *Forensic Science Providers: Codes of Practice and Conduct*. U.K. Crown. Available at: https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2016 (Accessed: 21 June 2016).

Freiling, C. and Schwittay, B. (2007). 'A Common Process Model for Incident Response and Computer Forensics', *3rd International Conference on IT-Incident Management & IT-Forensics*, pp. 19–40.

Frye v. United States, 54 App. D.C. 46, 293 F.1013 (1923).

Frey, T. (2013). *Hypermodelling: Next Level Software Engineering with Data Warehouses*. PhD thesis. Otto-von-Guericke-University Magdeburg.

Frowen, A. (2009). Computer Forensics In The Courtroom: Is An IT Literate Judge And Jury Necessary For A Fair Trial?. Available at: http://realestatearticles4u.com/computer-forensics-in-the-courtroom-is-an-it-literate-judge-and-jury-necessary-for-a-fair-trial/ (Accessed: 17 June 2016).

Fulcher, J. and Hills, P (1996). 'Towards a Strategic Framework for Design Research', *Journal of Engineering Design*, 7(1), pp. 183-193.

Garfinkel, S., Farrell, P., Roussev, V. and Dinolt, G. (2009). 'Bringing science to digital forensics with standardized forensic corpora', *Digital Investigation*, 6, pp.2–11.

Garfinkel, S. (2010). 'Digital forensics research: The next 10 years', *Digital Investigation*, 7, pp. 64–73.

Garber, L. (2001). 'Computer Forensics: High-Tech Law Enforcement', *IEEE Computer Magazine*, 34(1), pp. 22-27.

Garrie, D. (2014). 'Digital Forensic Evidence in the Courtroom: Understanding Content and Quality', *Northwestern Journal of Technology and Intellectual Property*, 12(2), pp. [i]-128.

Giova, G. (2011). 'Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems', *International Journal of Computer Science and Network Security*, 11(1), pp.1–9.

Gonzales, A., Schofield, R. and Hagy, D. (2007). *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/211314.pdf (Accessed: 17 June 2016).

Great Britain. *Computer Misuse Act 1990: Elizabeth II. Chapter 18* (1990). London: The Stationary Office.

Great Britain. *Criminal Justice Act 2003*: *Elizabeth II. Chapter 44* (2003). London: The Stationary Office.

Great Britain. *Police and Criminal Evidence Act 1984*: *Elizabeth II. Chapter 60* (1984). London: The Stationary Office.

Great Britain. *Regulation of Investigatory Powers Act 2000*: *Elizabeth II. Chapter 23* (2000). London: The Stationary Office.

Grobler, C.P., Louwrens, C.P. and Solms, S.H. (2010). 'A Multi-component View of Digital Forensics', *ARES '10 International Conference on Availability, Reliability and Security*, pp. 647-652.

Groesser, S. and Schwaninger, M. (2012). 'Contributions to model validation: hierarchy, process, and cessation', *System Dynamics Review*, 28(2), pp. 157-181.

Guidance Software. (2016). EnCase Forensics. Available at: https://www.guidancesoftware.com/encase-forensic (Accessed: 11 June 2016).

Harrison, W., Heuston, G., Morrissey, M., Aucsmith, D., Mocas, S. and Russelle, S. (2002). 'A Lessons Learned Repository for Computer Forensics', *International Journal of Digital Evidence*, 1(3), pp. 1-9.

Hauck, R., Atabakhsh, H., Ongvasith P., Gupta, H. and Chen, H. (2002). 'Using Coplink to analyze criminal-justice data', *IEEE Computer,* 35(3), pp. 30-37.

Hevner A., March, S., Park, J. and Ram, S. (2004). 'Design Science in Information Systems Research', *MIS Quarterly*, 28(1), pp. 75–105.

Hevner, A. and Chatterjee, S. (2010). *Design Research in Information Systems*. New York: Springer.

Hokstad, P., Oien, K. and Reinertsen, R. (1998). 'Recommendations on the use of expert judgment in safety and reliability engineering studies: two offshore case studies', *Reliability Engineering and System Safety*, 61(1), pp. 65-76.

Holden, M. and Lynch, P. (2004). 'Choosing the Appropriate Methodology: Understanding Research Philosophy', *The Marketing Review*, 4(4), pp. 397-409.

Holder, E., Robinson, L. and Rose, K. (2009). *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*, U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/227050.pdf (Accessed: 11 June 2016).

Ieong, R. (2006). 'FORZA - Digital forensics investigation framework that incorporate legal issues', *Digital Investigation*, 3, pp. 29–36.

IP Location. (2016). Where is Geolocation of an IP Address?. Available at: https://www.iplocation.net/ (Accessed: 11 June 2016).

International Organisation for Standardization. (2005). ISO/IEC 17799:2005. *Information technology -- Security techniques -- Code of practice for information security management.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2010). ISO/IEC 10118-2:2010. *Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2011). ISO/IEC 27035:2011. *Information technology -- Security techniques -- Information security incident management.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2012). ISO/IEC 27037:2012. *Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2013). ISO/IEC 27001:2013. *Information technology -- Security techniques -- Information security management systems -- Requirements.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2015). ISO/IEC 27041:2015. *Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2015). ISO/IEC 27042:2015. *Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence.* Geneva, Switzerland: International Organization for Standardization.

International Organisation for Standardization. (2015). ISO/IEC 27043:2015. *Information technology -- Security techniques -- Incident investigation principles and processes.* Geneva, Switzerland: International Organization for Standardization.

Jones, K., Bejtlich, R. and Rose, C. (2005). *Real Digital Forensics: Computer Security and Incident Response*. Boston: Addison-Wesley.

Jones, A. (2009) 'Computer Science and the Reference Manual for Scientific Evidence: Defining the Judge's Role as a Firewall', *Intellectual Property Law Bulletin*, 14(1), pp. 23-40.

Karyda, M. and Mitrou, L. (2007). 'Internet Forensics: Legal and Technical Issues', 2nd *International Workshop on Digital Forensics and Incident Analysis*, pp. 3-12.

Kelly, L. (2010). Provided Notes as an Alternative to Juror Notetaking: The Effects of Deliberation & Trial Complexity. Available at: http://eprints.utas.edu.au/10767/ (Accessed: 28 June 2016).

Kenneally, E. E. (2005). 'Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection', *UCLA Journal of Law and Technology*, 5, pp. 1-27.

Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. U.S. Department of Commerce. Available at: http://cybersd.com/sec2/800-86Summary.pdf (Accessed: 16 June 2016).

Kerr, O. (2009). *Computer Crime Law*. 2nd edn. St. Paul: Thomson/West.

Kerr, O. S. (2010). 'Fourth Amendment Seizures of Computer Data', *The Yale Law Journal*, 119(4), pp. 700-724.

Kessler, C. (2010). *Judges' Awareness, Understanding, and Application of Digital Evidence*. PhD thesis, Nova Southeastern University.

Khatir, M., Hejazi, M. and Sneiders, E. (2008). 'Two-dimensional evidence reliability amplification process model for digital forensics', *Third International Annual Workshop on Digital Forensics and Incident Analysis*, pp.21–29.

Kohn, M., Eloff, J. and Olivier, M. (2006). 'Framework for a Digital Forensic Investigation', *Information Security South Africa Conference*, pp. 1-7.

Kohn, M., Eloff, J. and Olivier, M. (2008). 'UML Modelling of Digital Forensic Process Models (DFPMs)', *ISSA Innovative Minds Conference*, pp. 1-13.

Kohn, M., Eloff, M. and Eloff, J. (2013). 'Integrated digital forensic process model', *Computers & Security*, 38, pp. 103–115.

Kruse, W. and Heiser, J. (2001). *Computer Forensics: Incident Response Essentials*. Boston: Addison-Wesley.

Kuechler, B. and Vaishnavi, V. (2008). 'On theory development in design science research: anatomy of a research project'. *European Journal of Information Systems*, 17(5), pp. 489-504.

Kuhnert, P., Martin, T. and Griffiths, S. (2010). 'A guide to eliciting and using expert knowledge in Bayesian ecological models', *Ecology Letters*, 13(7), pp. 900-914.

Kumho Tire v. Carmichael (1999). 526 U.S. 137, 119 S. *Ct, 1167(1169)*, p.143.

Law, A. (2014). *Simulation Modeling and Analysis.* 5th edn. McGraw-Hill.

Lawton, D., Stacey, R. and Dodd, G. (2014). *eDiscovery in digital forensic investigations*. Home Office. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf (Accessed: 16 June 2016).

Leigland, L. and Krings, A. (2004). 'A formalization of digital forensics', *International Journal of Digital Evidence*, 3(2), pp.1–32.

Losavio, M., Wilson, D. and Elmaghraby, A. (2006). Prevalence, Use, and Evidentiary Issues of Digital Evidence of Cellular Telephone Consumer and Small-Scale Digital Devices. *Journal of Digital Forensic Practice*, 1(4), pp. 291-296.

Ludwig, D., Mangel, M. and Haddad, B. (2001). 'Ecology, Conservation, and Public Policy', *Annual Review of Ecology and Systematics*, 32, pp. 481-517.

Mandia, K., Prosise, C. and Pepe, M. (2003). *Incident Response and Computer Forensics*. 2nd edn. Emeryville: McGraw-Hill/Osborne.

Manes, G., Downing, E., Watson, L. and Thrutchley, C. (2007). 'New Federal Rules and Digital Evidence', *Conference on Digital Forensics, Security and Law*, pp. 31-40.

Marcella, A. and Menendez, D. (2007). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. 2nd edn. Boston: Auerbach Publications.

March, S. and Smith, G. (1995). 'Design and natural science research on information technology', *Decision Support Systems*, 15 (4), pp.251-266.

March, S. and Storey, V. (2008). 'Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research', *MIS Quarterly*, 32 (4), pp. 725-730.

Markus, L., Majchrzak, A. and Gasser, L. (2002). 'A Design Theory for Systems That Support Emergent Knowledge Processes', MIS *Quarterly*, 26 (3), pp. 179-212.

Martin, T., Burgman, M., Fidler, F., Kuhnert, P., Low-choy, S., McBride, M. and Mengersen, K. (2012). 'Eliciting Expert Knowledge in Conservation Science', Conservation Biology, 26(1), pp. 29-38.

Mason, S. (2007). *Electronic Evidence: Disclosure, Discovery and Admissibility*. London: LexisNexis Butterworths.

McBride, M. and Burgman, M. (2012). 'What Is Expert Knowledge, How Is Such Knowledge Gathered, and How Do We Use It to Address Questions in Landscape Ecology?', *Expert Knowledge and Its Application in Landscape Ecology*, pp. 11-38.

McKemmish, R. (1999). *What is Forensic Computing?*. Australian Institute of Criminology. Available at: http://aic.gov.au/media_library/publications/tandi_pdf/tandi118.pdf (Accessed: 16 June 2016).

Memon, A., Vrij, A. and Bull, R. (2003). *Psychology and Law: Truthfulness, Accuracy and Credibility*. West Sussex: John Wiley & Sons.

Mercuri, R. (2005). 'Challenges in forensic computing', *Communications of the ACM*, 48(12), pp. 17-21.

Meyers, M. and Rogers, M. (2004). 'Computer forensics: The Need for Standardization and Certification', *International Journal of Digital Evidence*, 3(2), pp. 1-11.

Meyers, M. and Rogers, M. (2006). 'Digital Forensics: Meeting the Challenges of Scientific Evidence', *IFIP International Conference on Advances in Digital Forensics*, pp. 43-50.

Montasari, R., Peltola, P. and Carpenter, V. (2016). 'Gauging the Effectiveness of Computer Misuse Act in Dealing with Cybercrimes', *International Conference on Cyber Security and Protection of Digital Services,* pp. 1-5.

Montasari, R (2016, a). 'An Ad Hoc Detailed Review of Digital Forensic Investigation Process Models', *International Journal of Electronic Security and Digital Forensics (IJESDF),* 8 (3), pp. 205-223.

Montasari, R (2016, b). 'A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensics Practice', *International Journal of Computer Science and Security (IJCSS),* 10 (2), pp. 69-87.

Montasari, R. (2016, c). 'A Comprehensive Digital Forensic Investigation Process Model', *International Journal of Electronic Security and Digital Forensics (IJESDF),* 8 (4), pp. 285-301.

Montasari, R., Peltola, P. and Evans, D. (2015). 'Integrated Computer Forensics Investigation Process Model (ICFIPM) for Computer Crime Investigations', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 83-95.

Montasari, R. and Peltola, P. (2015). 'Computer Forensic Analysis of Private Browsing Modes', *Proceedings of 10th International Conference on Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security*, pp. 96-109.

Montasari, R. (in press). 'A Standardized Data Acquisition Process Model (SDAPM) for Digital Forensic Investigations', *International Journal of Information and Computer Security (IJICS)*.

Morgan, M and Henrion, M. (2010). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis.* New York: Cambridge University Press.

Mukasey, M., Sedgwick, J. and Hagy, D. (2008). *Electronic Crime Scene Investigation: A Guide for First Responders*. U.S. Department of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf (Accessed: 10 June 2016).

Mumba, E. and Venter, H. (2014). 'Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigations', *ADFSL Conference on Digital Forensics, Security and Law*, pp. 83-97.

Nance, K., Hay, B. and Bishop, M. (2009). 'Digital Forensics: Defining a Research Agenda', *42nd Hawaii International Conference on System Sciences*, pp.1–6.

Newman, R. (2007). 'Covert Computer and Network Communications', *4th annual Conference on Information Security Curriculum Development*, pp. 1-8.

NIST. (2015). *Computer Forensics Tool Testing Handbook*. U.S. Department of Commerce. Available at: http://www.cftt.nist.gov/CFTT-Booklet-08112015.pdf (Accessed: 16 June 2016).

Noblett, M., Pollitt, M. and Presley, L. (2000). 'Recovering and Examining Computer Forensic Evidence', *Forensic Science Communication*, 2(4), pp. 1-13.

Nunamaker, J., Chen, M. and Purdin, T. (1990). 'Systems Development in Information Systems Research', *Journal of Management Information Systems*, 7(3), pp. 89-106.

Ogloff, J., Clough, J., & Goodman-Delahunty, J. (2006). The Jury Project: Stage 1 – A Survey of Australian and New Zealand Judges. Available at: http://www.aija.org.au/online/Pub%20no77.pdf (Accessed: 28 June 2016).

OMG (2016). Unified Modeling Language (UML). Available at: http://www.omg.org/spec/UML/ (Accessed: 16 June 2016).

Ormerod, D. and Perry, D. (2015). *Blackstone's Criminal Practice*. 26th edn. Oxford: Oxford University Press.

Osterwalder, A. (2004). *The Business Model Ontology: A Proposition in a Design Science Approach*. PhD thesis. University of Lausanne.

Oxford Dictionaries. (2016). Harmonise. Available at: http://www.oxforddictionaries.com/definition/english/harmonize?q=harmonise (Accessed: 28 June 2016).

Pace, D. and Sheehan, J. (2002). 'Subject Matter Expert (SME)/Peer Use in M&S V&V', *21st Century workshop*, pp. i-34.

Parsonage, H. (2009). Computer Forensics Case Assessment and Triage. Available at: http://computerforensics.parsonage.co.uk/triage/triage.htm (Accessed: 16 June 2016).

Pearce J., Cherry K., Drielsma M., Ferrier S. and Whish, G. (2001), 'Incorporating expert opinion and fine-scale vegetation mapping into statistical models of faunal distribution, *Journal of Applied Ecology*, 38(2), pp. 412-424.

Peffers, K., Tuunanen, T., Gengler, C., Rossi, M., Hui, W., Virtanen, V. and Bragge, J. (2006). 'The Design Science Research Process: A Model for Producing and Presenting Information Systems Research', *1st International Conference on Design Science Research in Information Systems and Technology*, pp. 83-106.

Palmer, G. (2001). 'A Road Map for Digital Forensic Research', *1st Digital Forensic Research Workshop (DFRWS)*, pp.27–30.

Perumal, S. (2009). 'Digital Forensic Model Based On Malaysian Investigation Process', *International Journal of Computer Science and Network Security*, 9(8), pp. 38-44.

Peisert, S., Bishop, M. and Marzullo, M. (2008). 'Computer Forensics in Forensics', *Third International Workshop on Systematic Approaches to Digital Forensic Engineering,* pp. 102-122.

Pollitt, M. (2007). 'An Ad Hoc Review of Digital Forensic Models', *2nd International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 43-54.

Pollitt, M. (2009). 'The Good, the Bad, the Unaddressed', *Journal of Digital Forensic Practice*, 2(4), pp. 172-174.

Pollitt, M. (2010). 'A History of Digital Forensics', *IFIP Advances in Information and Communication Technology*, pp. 3-15.

Reich, Y. (1994). 'The Study of Design Methodology', *Journal of Mechanical Design*, 117 (2), pp. 211-214.

Reith, M., Carr, C. and Gunsch, G. (2002). 'An Examination of Digital Forensic Models', *International Journal of Digital Evidence*, 1(3), pp. 1-12.

Rocco, T. and Hatcher, T. (2011). *The Handbook of Scholarly Writing and Publishing*. San Francisco: John Wiley & Sons.

Rogers, M. (2004). *DCSA: A Practical Approach to Digital Crime Scene Analysis*. 5th edn. Vol. 3, West Lafayette, Purdue University, USA.

Rogers, M., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006). 'Computer Forensics Field Triage Process Model', *Conference on Digital Forensics, Security and Law*, pp. 27-40.

Rogers, M., Scarborough, K., Frakes, K. and San Martin, C. (2007). 'Survey of Law Enforcement Perceptions Regarding Digital Evidence', *IFIP International Conference on Digital Forensics in Advances in Digital Forensics*, pp. 41-52.

Rossi, M. and Sein, M. (2003). 'Design research workshop: a proactive research approach', *26th Information Systems Research Seminar in Scandinavia*, pp. 9-12.

Rothlisberger, J., Lodge, D., Cooke, R. and Finnoff, D. (2010). 'Future declines of the binational Laurentian Great Lakes fisheries: the importance of environmental and cultural change', *Frontiers in Ecology and the Environment*, 8(5), pp. 239-244.

Rothstein, B., Hedges, R. and Wiggins, E. (2007). Managing Discovery of Electronic Information: A Pocket Guide for Judges. Available at: https://bulk.resource.org/courts.gov/fjc/eldscpkt.pdf (Accessed: 21 June 2016).

Rowlingson, R. (2004). 'A Ten Step Process for Forensic Readiness', *International Journal of Digital Evidence*, 2(3), pp. 1-28.

Ruan, C. and Huebner, E. (2009). 'Formalizing Computer Forensics Process with UML', *3rd International Conference on Information Systems: Modeling, Development, and Integration*, pp. 184-189.

Ryan, D. and Shpantzer, G. (2002). 'Legal Aspects of Digital Forensics', *Proceedings of Forensics Workshop*, pp. 1-7.

Saferstein, R. (2010). *Criminalistics: An Introduction to Forensic Science*. 10th edn. Prentice Hall.

Sammes, A. and Jenkinson, B. (2007). *Forensic Computing: A Practitioner's Guide*. 2nd edn. London: Springer.

Scarborough, E., Rogers, M., Frakes, K. and San Martin, C. (2009). 'Digital Evidence', *Crimes of the Internet,* pp. 477-488.

Selamat, S., Yusof, R. and Sahib, S. (2008). 'Mapping Process of Digital Forensic Investigation Framework', *International Journal of Computer Science and Network Security*, 8(10), pp. 163-169.

Shaw, B. (2006). 'Judging Juries: Evaluating Renewed Proposals for Specialized Juries From a Public Choice Perspective', *UCLA Journal of Law and Technology*, 10(2), pp. 3-4.

Sherman, S. (2006). 'A digital forensic practitioner's guide to giving evidence in a court of law', *Proceedings of the 4th Australian Digital Forensics Conference*, pp. 1-7.

Smith, R., Grabosky, P. and Urbas, G. (2011). *Cyber Criminals on Trial*, Cambridge: Cambridge University Press.

Solomon, M., Rudolph, K., Tittel, E., Broom, N. and Barrett, D. (2011). *Computer Forensics JumpStart*. 2nd edn. Indianapolis: Wiley Publishing.

Sommer, P. (2008). *Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence*. U.K. Information Assurance Advisory Council. Available at: https://www.ucisa.ac.uk/~/media/Files/members/activities/ist/DigitalInvestigationsGuide.ashx (Accessed: 17 June 2016).

Sommerville, I. and Sawyer, P. (1997). 'Viewpoints: Principles, Problems and a Practical Approach to Requirements Engineering', *Annals of Software Engineering*, 3(1), pp. 101-130.

Stanfield, A. (2009). *Computer Forensics, Electronic Discovery and Electronic Evidence*. Chatswood: LexisNexis Butterworths.

Steel, C. (2006). *Windows Forensics: The Field Guide for Conducting Corporate Computer Investigations*. Indianapolis: Wiley Publishing.

Sutherland, W. (2006). 'Predicting the ecological consequences of environmental change: a review of the methods', *Journal of Applied Ecology*, 43(4), pp. 599-616.

Sutherland, W. (2008). 'Predicting the ecological consequences of environmental change: a review of the methods', *Journal of Applied Ecology*, 43(4), pp. 599-616.

Takeda, H., Veerkamp, P., Tomiyama, T. and Yoshikawa, H. (1990). 'Modeling Design Processes', *AI Magazine*, 11(4), pp. 37-48.

Tan, J. (2001). Forensic Readiness. Available at: https://isis.poly.edu/kulesh/forensics/docs/forensic_readiness.pdf (Accessed: 17 June 2016).

TheFreeDictionary. (2016). Harmonise. Available at: http://www.thefreedictionary.com/Harmonise (Accessed: 28 June 2016).

Trcek, D., Abie, H., Skomedal, A. and Starc, I. (2010). 'Advanced Framework for Digital Forensic Technologies and Procedures', *Journal of Forensic Sciences*, 55(6), pp. 1471–1480.

US-CERT. (2012). *Computer Forensics*. U.S. Department of Homeland Security. Available at: https://www.us-cert.gov/security-publications/computer-forensics (Accessed: 17 June 2016).

U.S. Courts. (2015). *Federal Rules of Evidence*. Administrative Office of the U.S. Courts. Available at: http://federalevidence.com/rules-of-evidence (Accessed: 21 June 2016).

Vaishnavi, V. and Kuechler, B. (2004). Design Research in Information Systems. Available at: http://www.desrist.org/design-research-in-information-systems/ (Accessed: 17 June 2016).

Valjarevic, A. and Venter, H. (2012). 'Harmonised Digital Forensic Investigation Process Model', *Proceedings of Information Security for South Africa*, pp.1-10.

Valjarevic, A. and Venter, H. (2015). 'A Comprehensive and Harmonized Digital Forensic Investigation Process Model', *Journal of Forensic Sciences*, 60(6), pp. 1467-1483.

Venter, J. (2006). Process Flow for Cyber Forensics Training and Operations. Available at: http://researchspace.csir.co.za/dspace/handle/10204/1073 (Accessed: 17 June 2015).

von Solms, S., Louwrens, C., Reekie, C. and Grobler, T. (2006). 'A Control Framework for Digital Forensics', *IFIP International Conference on Advances in Digital Forensics*, pp. 343-355.

Walls, J., Widmeyer, G. and El Sawy, O. (1992). 'Building an Information System Design Theory for Vigilant EIS', *Information Systems Research*, 3(1), pp. 36-59.

Walls, J., Widmeyer, G. and El Sawy, O. (2004). 'Assessing Information System Design Theory in Perspective: How Useful Was Our 1992 Initial Rendition?', *Journal of Information Technology Theory and Application (JITTA*), 6(2), pp.43-58.

Watts, S., Shankaranarayanan, G. and Even, A. (2009). 'Data quality assessment in context: A cognitive perspective', *Decision Support Systems*, 48 (1), pp. 202-211.

WhatIsMyIPAddress. (2016). How you connect to the world. Available at: http://whatismyipaddress.com/ (Accessed: 17 June 2016).

Whitcomb, C. (2002). 'An Historical Perspective of Digital Evidence: A Forensic Scientist's View', *International Journal of Digital Evidence*, 1(1), pp. 1-9.

Whitfield, P., Ruddock M, Bullman, R. (2008). 'Expert opinion as a tool for quantifying bird tolerance to human disturbance', *Biological Conservation*, 141(11), pp. 2708-2717.

Wieringa, R. (2009). 'Design Science as Nested Problem Solving', *4th International Conference on Design Science Research in Information Systems and Technology*, pp. 8-19.

Wiles, J. (2007). *The Best Damn Cybercrime and Digital Forensics Book Period*. USA: Syngress.

Wise, J., Hopkin, D. and Stager, P. (2013). *Verification and Validation of Complex Systems: Human Factors Issues*. Berlin: Springer-Verlag.

Wojcik, M., Venter, H., Eloff, J. and Olivier, M. (2006). 'Applying Machine Trust Models to Forensic Investigations', *IFIP international Conference on Advances in Digital Forensics*, pp. 55-65.

Yeschke, C. (2002). *The Art of Investigative Interviewing: A Human Approach to Testimonial Evidence*. 2nd edn. Boston: Butterworth-Heinemann.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011). 'Common Phases of Computer Forensics Investigation Models', *International Journal of Computer Science & Information Technology*, 3(3), pp. 17-31.

Zainudin, N., Merabti, M. and Llewellyn-Jones, D. (2011). 'Online Social Networks As Supporting Evidence: A Digital Forensic Investigation Model and Its Application Design', *International Conference on Research and Innovation in Information Systems*, pp. 1-6.

Appendix A. Forensic Laboratory Experimentation

This section discusses the practical experimentation of the Demonstration activity that was carried out in a digital forensic laboratory (DFL)[44]. Under the experimentation approach, the thesis author would act as a DFI commissioned to conduct a hypothetical digital investigation and present its findings in the form of a 'formal report' to be submitted in a court of law. The aim of this approach is to demonstrate essential investigative techniques associated with the Investigative Processes Class of the CDFIPM, that could be used to answer the investigative questions of who, when, where and how. Since this report is embedded within the thesis, its structure (e.g. headings, numbering, and sections, etc.) does not fall under the thesis structure.

It is assumed that DFAs following the techniques outlined in the following report maintain a detailed note-taking during any forensic investigation. This is due to the fact that a successful digital investigation requires detailed notes during the course of an investigation. These notes can be in the form of taking photographs, videos and screen captures, bookmarking the digital evidence through a forensic software tool such as Encase, FTK and XWays Forensics etc., utilising built-in logging/reporting options within the forensic software tool, highlighting and exporting data (representing potential digital evidence) into for example, .CSV, .TXT, .XLSX and .PDF, .JPG, .PNG and .GIF files, or even a digital audio recorder as well as hand-written notes. There does not exist a standard requiring DFAs to follow a particular method when conducting the note-taking. This will depend on DFAs as each DFA might approach the note-taking process differently. However, the more notes a DFA takes, the easier it will become to prepare and finalize the report.

[44] The practical experimentation of the Demonstration activity was carried out in one of the digital forensic laboratories of the University of South Wales (formerly known as the University of Glamorgan) due to their extensive resources as well as well-equipped laboratories.

Report on Forensic Analysis of the Computer Allegedly Used to Penetrate BOLtd Network Security

DIGITAL FORENSIC ANALYST:	Digital Forensic Investigator, Reza Montasari
	Cheshire Headquarter Police High-Tec Crime Unit Clemonds Hey, Winsford, Cheshire, CW7 2UA Email: r.montasari@derby.ac.uk Phone: 0151 424 7431
INSTRUCTING PARTY:	Head of the Cheshire Headquarter Police High-Tech Crime Unit, Detective Sergeant Andrew Dodd
	Cheshire Headquarter Police High-Tec Crime Unit Clemonds Hey, Winsford, Cheshire, CW7 2UA Phone: 0151 424 7431
SUBJECT:	**Digital Forensic Expert Witness Report**
UK GUDILEINES ADHERED TO:	The Comprehensive Digital Forensic Investigation Process Model, the CDFIPM
CASE REFERENCE NUMBER:	100326837-BOLtd-Vindaloo-Hacking
REFERENCE ITEM:	HD Image (vindaloo_.E01 & vindaloo_.E02) - 19,077 MB
OFFENCE:	Illegal penetration into network system, Hacking and theft of proprietary information
ACCUSED:	Thomas Nigel
DATE OF REQUEST:	2nd November 2015
DATE OF CONCLUSION:	3rd June 2016

Statement of Truth:

I believe that the facts stated in this document are true. I testify that digital evidence (the hard drive image) received has not been altered in any way and the hard drive image has not been in any other individuals' possession during the period of 70 days (from 2nd March 2016 to 11th May 2016), during which the forensic analysis was carried out.

Notice: All technical terms in the report are highlighted in bold when first used. Explanations are provided in the Glossary of Terms (Appendix A.1).

A.1 Background to the Case

Board Optimisation (BO) Company, which specialises in the optimisation of **PCB board [1]** designs, believes a hacker has successfully penetrated their network security system, accessing a number of files including a design for a new PCB for a major entertainment system manufacturer. The Nottingham Headquarter Police Plaza traced the suspect and seized his/her computer, which was reportedly used to penetrate BOLtd's network. It is thought that this computer contains evidence related to this intrusion.

A.2 Executive Summary

Using different forensic tools and methodologies, seven factual and nine suspicious evidence items were discovered (see A.4.1 and A.4.2). Upon completing the Analysis Process, it appears that the suspect's system was used to penetrate into BOLtd's network. Documents belonging to BOLtd Company were discovered on the suspect's system. Based upon the log files discovered, it appears that WinSCP software was used for unauthorised file transfers. It also appears that the suspect was a student completing a university course, possibly in the area of digital forensic or network security, with a good understanding of Information Technology. Analysis revealed that the suspect was actively attempting to learn about tools and techniques regarding the exploitation of network security vulnerabilities. For example, tools were downloaded such as WinSCP and **Back Oriface [3]** etc. and five PDF files explaining penetration tools and techniques were discovered. Examining the Internet history of the browsers installed revealed that the suspect had visited and bookmarked certain questionable websites for information about hacking tools and techniques.

A.3 Objectives

On 2nd March 2016 at 13:00 PM, Detective Sergeant Huw Read contacted my office with regards to the examination and analysis of a computer's hard drive suspected of containing potential evidence associated with the penetration into BOLtd's network. He informed me that the suspect's computer had already been seized by the police officers in the division, and that another detective in our High-Tech Crime Unit, Mr. Gareth Davis, had already carried out the forensic data acquisition on the hard drive. Detective Sergeant Huw Read proceeded to provide me with the **hard drive image [2]** and commissioned a full forensic analysis as well as a report for possible criminal charges and civil litigation. The goal was to examine and analyse the hard drive image to identify and recover any evidence items related to BOLtd's network security breach. I shall therefore present my relevant findings in section A.4 of this report, while in section A.5, I shall discuss the steps that I took to conduct this digital forensic analysis. Finally, I will provide my conclusion in section A.7.

A.4 Relevant Findings

This section details the factual and suspicious items of evidence recovered from the hard drive image that have both probative and evidential value.

A.4.1 Factual Items

A.4.1.1 Evidence Item 1

Text file – evidence item: an email which appears to have circulated amongst two of the BOLtd's employees was found on the suspect's system. This was a deleted file recovered through **'Data Carving' [8]**. Analysing two recovered database log files entitled **'index.dat' [9]** and "NTUSER.DAT", it is suspected that WinSCP tool using Internet Explorer version 5 had been used to hack into a BOLtd computer to acquire the document (Refer to sections A.4.1.3, A. 4.1.4 and A.4.1.5 for information on these files). The file path to this evidence is: ***/img_vindaloo_.E01/$OrphanFiles/Bob.txt***

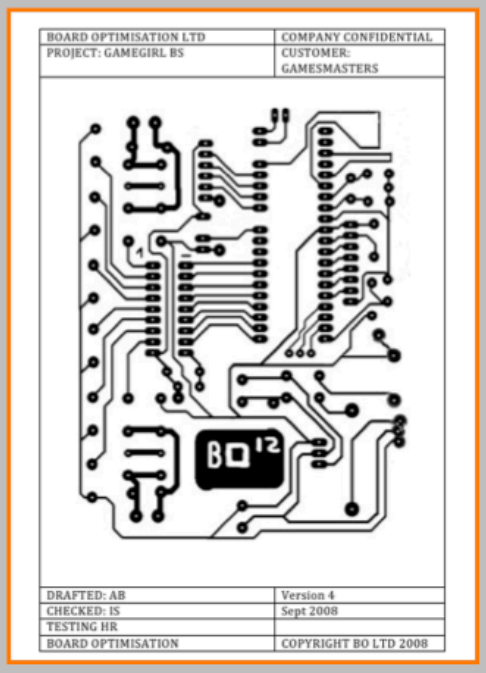
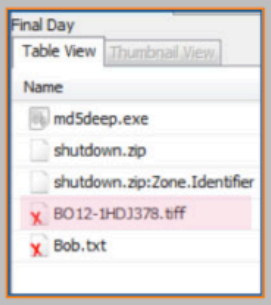
Table 4. Factual evidence item 1: text file

File Name:	Bob.txt	File Hash	MD5: BF77E010F189479BE19879E7620852A6 SHA1: F23D3774B026C48065CDB9D270A370AEFCFC8099
Evidence Item No:	N/A	Deleted?	Yes
Created Date:	24/11/2008 04:34:23	File Extension	Ok
Modified Date:	29/11/2009 21:07:18	Duplicate	No
Accessed Date:	24/11/2008 04:35:10	L/P Size	994/ 994
TXT File:	From: "Cash, Robert" Robert.Cash@Gamesmasters.com Date: Fri, 15 Aug 2008 11:39:34 +0000 To: ?Anthony Brush? <abrush@bo.co.uk> Subject: Gamegirl console Hi Robert, I am glad to hear that progress is going well on the new board design. This will give us quite an edge over our rivals in the size and cost of the device. I look forward to seeing the prototype. Please ensure the utmost secrecy is applied to both the specification and the board design. Best Regards Tony > From: "Brush, Anthony" <abrush@bo.co.uk> > Date: Thu, 14 Aug 2008 10:36:22 +0000 > To: Robert Cash <Robert.cash@gamesmasters.com > Subject: Gamegirl console > > Dear Tony > > We have completed the optimized layout of the secondary controls PCB for the gamegirl Controller >It appears we can reduce the size of the component to 2/3 original> >This will make a significant impact on cost >We are building a prototype for full testing later this week > > > Best wishes > > Bob Final Day Table View Thumbnail View Name md5deep.exe shutdown.zip shutdown.zip:Zone.Identifier BO12-1HDJ378.tiff Bob.txt		

A.4.1.2 Evidence Item 2

Image file – evidence item: a new PCB board confidential design: the suspect had deleted this; however, it was discovered through data carving. Similar to 'Evidence Item 1', analysing 'index.dat' and 'NTUSER.DAT', it appears that WinSCP was utilised with Internet Explorer Version 5 to hack the document (see sections A.4.1.3, A. 4.1.4 and A.4.1.5 for details). Also, a short-cut, 'BO12-1HDJ378.lnk' had been made. The file path to this file is: ***/img_vindaloo_.E01/$OrphanFiles/BO12-1HDJ378.tiff***

Table 5. Factual evidence item 2: image file

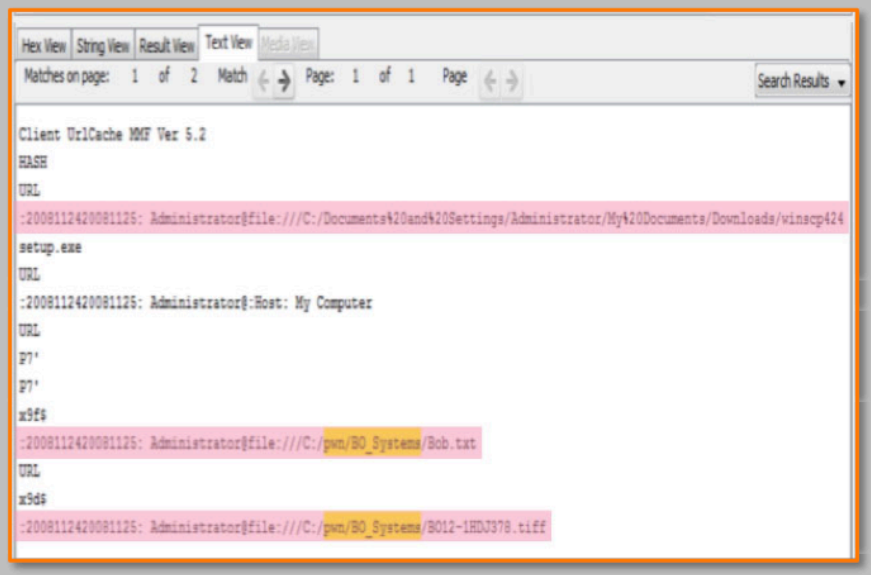
File Name:	BO12-1HDJ378.tiff	File Hash	MD5: 3C1CA8A67454A17AA58BD8DF3E52ABF9 SHA1: A3AD1845673DD50C2F36218C60EF1895267A5749
Evidence Item No:	N/A	Deleted?	Yes
Created Date:	24/11/2008 04:34:43	File Extension	Ok
Modified Date:	29/11/2009 21:07:45	Duplicate	No
Accessed Date:	24/11/2008 04:34:20	L/P Size	169,838/ 169,838
Image File:	 		

A.4.1.3 Evidence Item 3

Database file – evidence item: small-sized database file: Investigating the below 'index.dat' file, it appears that the suspect utilised WinSCP to penetrate the BOLtd's network and download evidence items 1 and 2 (see sections A. 4.1.5 and A.4.1.6). The path to the database file is:

Documents and Settings/Administrator/Local Settings/History/History.IE5/MSHist012008112420081125/index.dat

Table 6. Factual evidence item 3: database file

File Name:	index.dat	File Hash	MD5: A1D1C6DEECAE9C4480389F597DCBD3D7 SHA1: 2CB8CC759E23F122FD4ABE968BCC0661FC99DBC9
Evidence Item No:	N/A	Deleted?	No
Created Date:	24/11/2008 04:32:23	File Extension	OK
Modified Date:	24/11/2008 04:26:55	Duplicate	No
Accessed Date:	24/11/2008 04:32:23	L/P Size	32,768/ 32,768
Image File:			

A.4.1.4 Evidence Item 4 and 5

A Desktop Shortcut and a Database File – evidence items: Examining this file, it appears that the suspect had a shortcut to a directory 'C:\pwn" entitled "BO_Systems'. At first, it looks as though this is a shortcut to a remote machine (i.e. 'ADMIRALKIRK') but on closer inspection via the suspect's system registry, it was revealed that ADMIRALKIRK is the hostname of the suspect's computer.

The presence of this shortcut indicates that the suspect may have had content relating to BO Systems stored in C:\pwn.

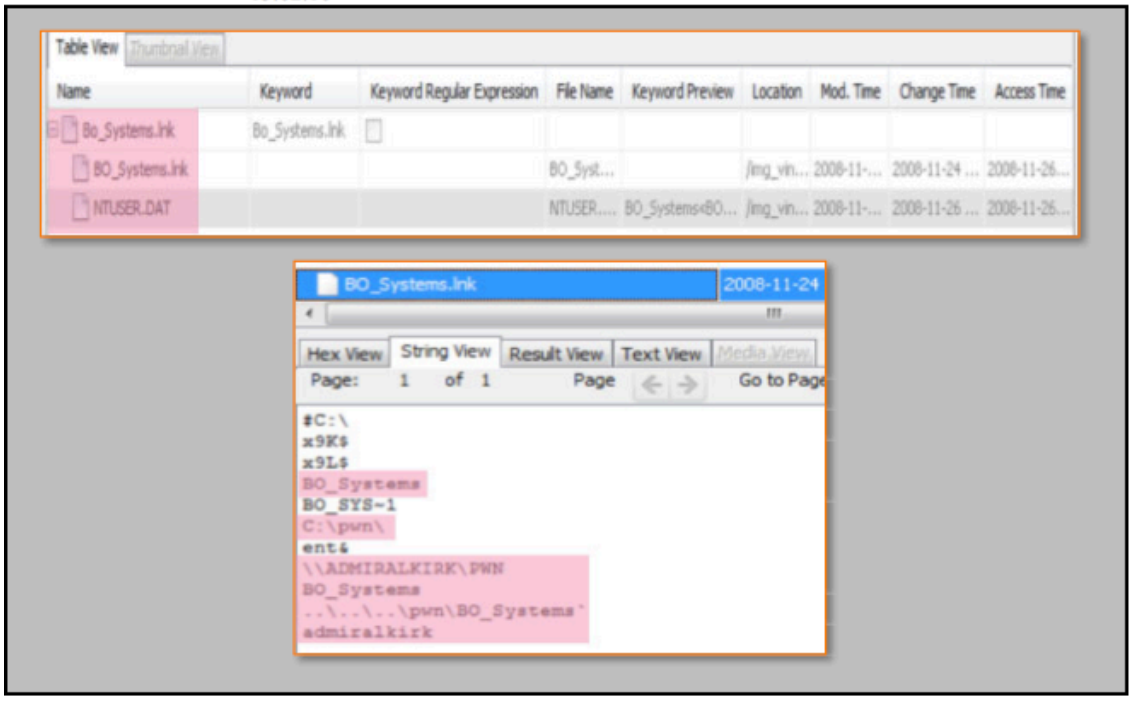
The file path to Bo_System.lnk is:

/img_vindaloo_.E01/Documents and Settings/Administrator/Recent/BO_Systems.lnk

The file path to NTUSER.DAT is:
/img_vindaloo_.E01/Documents and Settings/Administrator/NTUSER.DAT

Table 7. Factual evidence items 4 and 5: a desktop shortcut and a database file

File Name:	1-Bo_System.lnk 2-NTUSER.DAT	File Hash	1-MD5: BE8C8D0B15BB0DFF058616EB7DDB235E 1-SHA1: 21ED73B1B2459EBADB64B5B7341351466B15DECF 2-MD5: 496B839F2B1C20FC7F1683F5BB6FBB9B 2-SHA1: 222B3339C0F5957EE6A7952652C1340744F7D36E
Evidence Item No:	N/A	Deleted?	No
Created Date:	**1**-24/11/2008 04:34:43 **2**-14/11/2008 22:46:28	File Extension	OK
Modified Date:	**1**-24/11/2008 04:35:10 **2**-26/11/2008 13:02:10	Duplicate	No
Accessed Date:	**1**-26/11/2008 12:11:26 **2**-26/11/2008 13:02:10	L/P Size	1- 431/ 431 2- 487,424/ 487,424



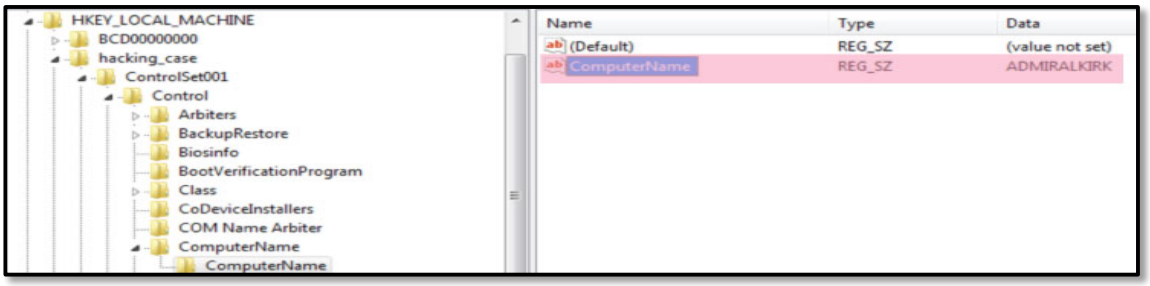


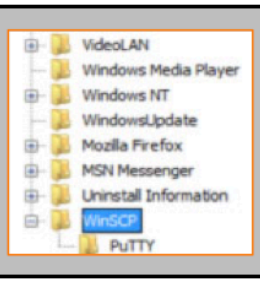
Figure 49. The suspect's "C:\WINNT\system32\config\system" registry hive loaded for investigation

A.4.1.5 Evidence Item 6

Executable file –evidence item– an **SFTP client** for Microsoft Windows: The main function of WinSCP is to secure file transfer between local and remote computers. Although used for legitimate reasons, such as enabling students to connect to their institution's servers, it can also be used for illegal penetration to a remote network. Examining a database **Log file [10]** entitled 'index.dat' (see evidence item A.4.1.3) suggested that the suspect might have used this program to penetrate into BOLtd's network (see A.4.1.6).

The path to the location of this program is: ***Program Files/WinSCP/WinSCP.exe***

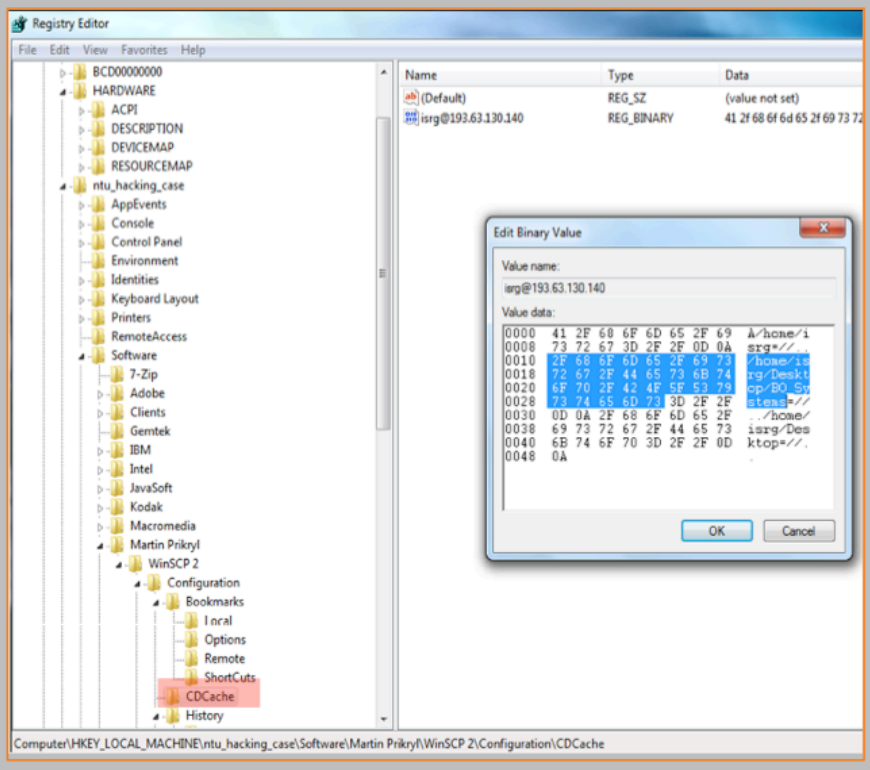
Table 8. Factual evidence item 6: executable file- an SFTP client for Microsoft Windows

File Name	WinSCP.exe	File Hash	MD5: BE8AE9338B77E8E7BC71A95D30A1AD5A SHA1: AD961E162246731F2DC04F2E3F62F44D6FEEE127
Evidence Item No	N/A	Deleted?	No
Created Date	24/11/2008 04:32:43	File Extension	OK
Modified Date	25/10/2008 20:16:06	Duplicate	No
Accessed Date	24/11/2008 04:32:46	L/P Size	6,345,216/ 6,345,216
			

A.4.1.6 Evidence Item 7

Registry Data – evidence item: WinSCP CDCache: Loading the user's registry hive (NTUSER.DAT in C:\Documents and Settings\Administrator) on the investigator's machine allowed for an in-depth view of system and application settings and other registry data. One such piece of data which could be recovered was the 'CDCache' of WinSCP – a location in the registry which is used by WinSCP to cache the directories used in a session. This data implies that a session has been opened using the username 'isrg' on the host '193.63.130.140' (which resolves to j4-phd04.fat.glam.ac.uk). At some point during the session, a directory at "/home/isrg/Desktop/BO_Systems" was opened.

Table 9. Factual evidence items 7: registry data- WinSCP CDCache

File Name:	WinSCP CDCache	File Hash	MD5: N/A SHA1: N/A
Evidence Item No:	N/A	Deleted?	N/A
Created Date:	N/A	File Extension	N/A
Modified Date:	N/A	Duplicate	N/A
Accessed Date:	N/A	L/P Size	N/A
Executable File:			

A.4.2 Suspicious Items of Evidence

A.4.2.1 Evidence Item 1

Evidence Item: MSN instant messages saved as XML file: Investigating the Log files of the **MSN Live Messenger**, it became clear that the suspect held conversations with someone appearing to be the suspect's friend. They discussed possible ways of penetrating another's computer. At the time of the conversations, both appeared to be students completing an assignment. The conversations were stored in a script on the suspect's system entitled "huwbear613786887.xml".

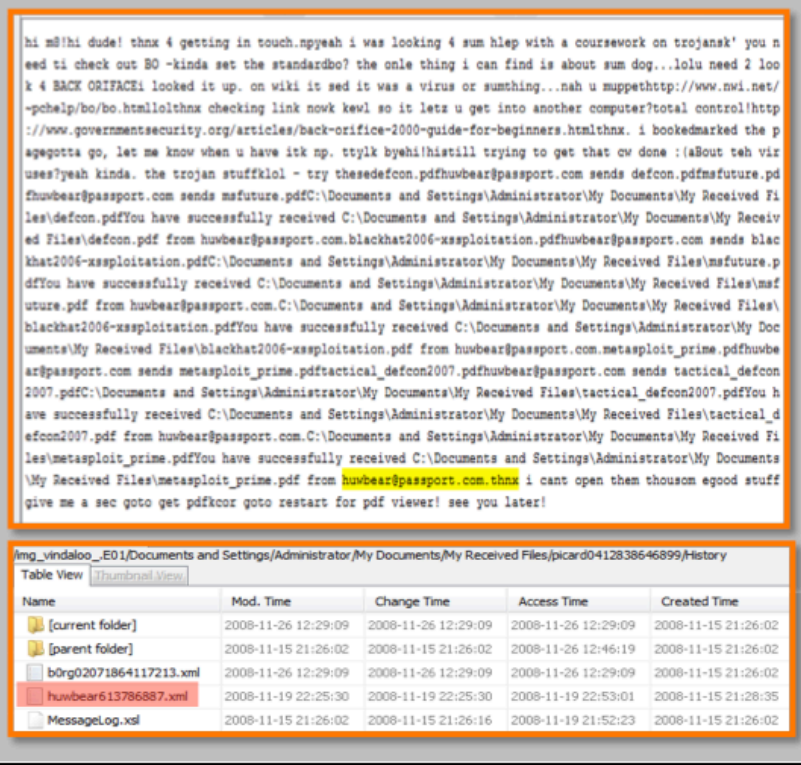
The full path to the location of this XML file is:

Documents and Settings/Administrator/My Documents/My Received Files/Pickard0412838646899/History/ HUWBEAR613786887.XML

Further investigation of this script and following the traces discovered revealed that the friend with the email address of 'huwbear@passport.com' had sent 5 PDF files containing information about how to penetrate and exploit network resources to the suspect, whose email address appeared to be 'picard012@passport.com'. The friend advised the suspect to look into 'Back Oriface', a tool which could be used to penetrate a network. Below sub-sections discuss these PDF files and Back Oriface.

Table 10. Suspicious evidence item 1: MSN instant messages saved as XML file

File Name	huwbear613786887.xml	File Hash	MD5: 462B1CF95A1A90CDF87D06FB94C48830 SHA1: D87C52C8FA6F61A1CB0614F315474F194BA903D9
Evidence Item No	N/A	Deleted?	No
Created Date	15/11/2008 21:28:35	File Extension	OK
Modified Date	19/11/2008 22:25:30	Duplicate	No
Accessed Date	19/11/2008 22:53:01	L/P Size	13,478/ 13,478
Image File			



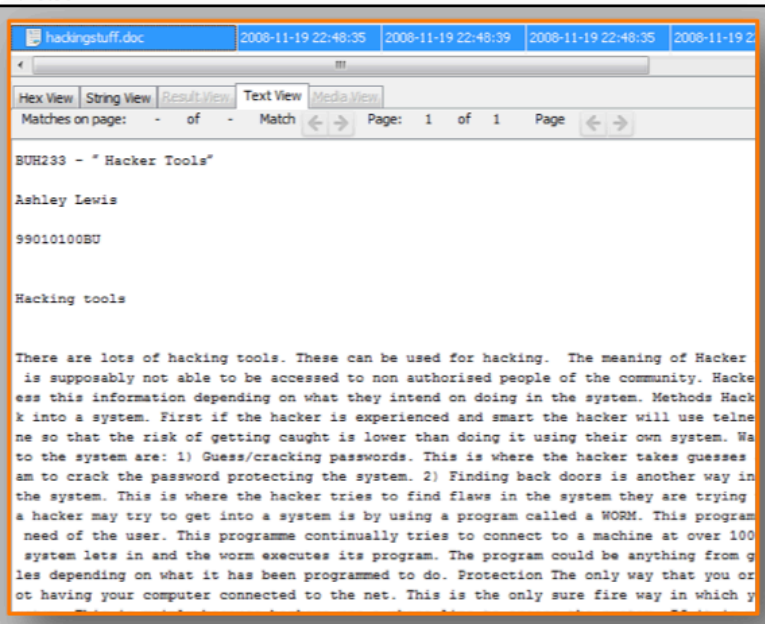
A.4.2.2 Evidence Item 2

Doc File – Evidence Item: hackingstuff: The above discovered evidence again suggests that the suspect had looked into hacking information and had a good understanding of network penetration. This document appears to be an assignment completed by the suspect and suggests the suspect was a student.

The file path is:

/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/uni cw/hackingstuff.doc

Table 11. Suspicious evidence item 2: doc file

File Name:	Hackingstuff.doc	File Hash	MD5: B24333715D13F532B6D0AF5B5168AF24 SHA1: 123F8D64B4F79DFEC82919F6D413C79A6DA66784
Evidence Item No:	N/A	Deleted?	No
Created Date:	19/11/2008 22:40:41	File Extension	OK
Modified Date:	19/11/2008 22:48:35	Duplicate	No
Accessed Date:	19/11/2008 22:48:35	L/P Size	22,016/ 22,016
Executable File:			

A.4.2.3 Evidence Item 3, 4, 5, 6 and 7

Evidence Items: Five PDF files: All PDF files were stored in 'My Received Files' folder, a default folder for MSN messenger to store received files. The file paths to these PDF files are:

msfuture.pdf
/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/msfuture.pdf

defcon.pdf
/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/defcon.pdf

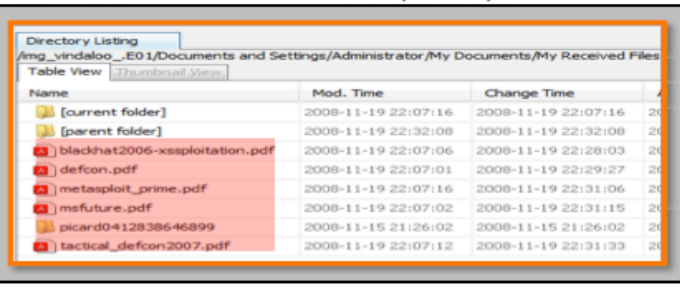
blackhat2006-xssploitation.pdf
/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/blackhat2006-xssploitation.pdf

metasploit_prime.pdf
/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/metasploit_prime.pdf

tactical_defcon2007.pdf
/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/tactical_defcon2007.pdf

Table 12. Suspicious evidence items 3, 4, 5, 6 and 7: five PDF files

File Name	**1-** msfuture.pdf **2-** defcon.pdf **3-** blackhat2006-xssploitation.pdf **4-** metasploit_prime.pdf **5-** tactical_defcon2007.pdf	File Hash	**1-** MD5: 032E9D59CB21D909478B02788ED81E46 **1-** SHA1: D5A428821668EDF88FF0A20AEDEE12132415EFAD **2-** MD5: AC49EA330FE295BD52F81AF91F3BF699 **2-** SHA1: E71626543202A1DA7F1FCFC1853C04C26196E35B **3-** MD5: BC81E4C752A992DE5D3E755849978A15 **3-** SHA1: 39B2CB0514620AB9501ED4E69AAB1E4CDDD6529A **4-** MD5: 9DD57D771F26E07944366453D93401D9 **4-** SHA1: 5B38523971F548FD5D5E79D6301F05FBB0CD607D **5-** MD5: BE60D69EA94099912ECFCBE2585347E8 **5-** SHA1: 23803F84AF91C683A6953819292C8A88C6E36936
Evidence Item No	N/A	Deleted?	**1-** No **2-** No **3-** No **4-** No **5-** No
Created Date	**1-** 19/11/2008 – 22:06:58 **2-** 19/11/2008 – 22:06:57 **3-** 19/11/2008 – 22:07:05 **4-** 19/11/2008 – 22:07:15 **5-** 19/11/2008 – 22:07:11	File Extension	**1-** OK **2-** OK **3-** OK **4-** OK **5-** OK
Modified Date	**1-** 19/11/2008 – 22:07:02 **2-** 19/11/2008 – 22:07:01 **3-** 19/11/2008 – 22:07:06 **4-** 19/11/2008 – 22:07:16 **5-** 19/11/2008 – 22:07:12	Duplicate	**1-** No **2-** No **3-** No **4-** No **5-** No
Accessed Date	**1-** 19/11/2008 – 22:47:32 **2-** 19/11/2008 – 23:31:01 **3-** 19/11/2008 – 22:46:28 **4-** 19/11/2008 – 22:46:33 **5-** 19/11/2008 – 22:48:41	L/P Size	**1-** 365,116/ 365,116 **2-** 265,269/ 265,269 **3-** 630,242/ 630,242 **4-** 148,889/ 148,889 **5-** 320,062/ 320,062



A.4.2.4 Evidence Item 8

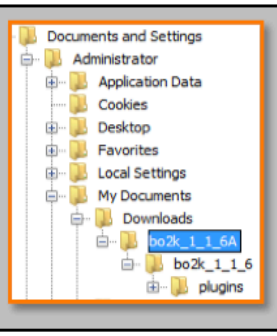
Executable File – Evidence Item: Back Oriface: Using Mozilla Firefox, the suspect downloaded BO2K from the website 'sourceforge' onto the 'Downloads' folder. The path is: ***/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/Downloads/bo2k_1_1_6A/BO2K_1-1_6/***

However, there was not enough evidence to suggest the suspect had installed this software on his machine; except the fact that there was a shortcut icon called 'b2ok.lnk' on his desktop to this executable program. This tool can be deployed by cyber-

criminals to penetrate a network. Entries of this executable file could be found in downloads.sqlite. The path is:

/img_vindaloo_.E01/Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/downloads.sqlite

Table 13. Suspicious evidence item 8: Back Oriface

File Name:	Bo2k.exe	File Hash	MD5: D8A3CE18770682848678F279196E8D39 SHA1: 7816077A6B8C26F536775DFB4D4E1C8680AF5488
Evidence Item No:	N/A	Deleted?	No
Created Date:	19/11/2008 22:49:12	File Extension	OK
Modified Date:	19/11/2008 22:49:13	Duplicate	No
Accessed Date:	26/11/2008 12:29:45	L/P Size	196,608/ 196,608
Executable File:			

B2OK had been deleted. An entry for the deletion of this software could be seen in the 'Recycler'. (see section A.5.3.4)

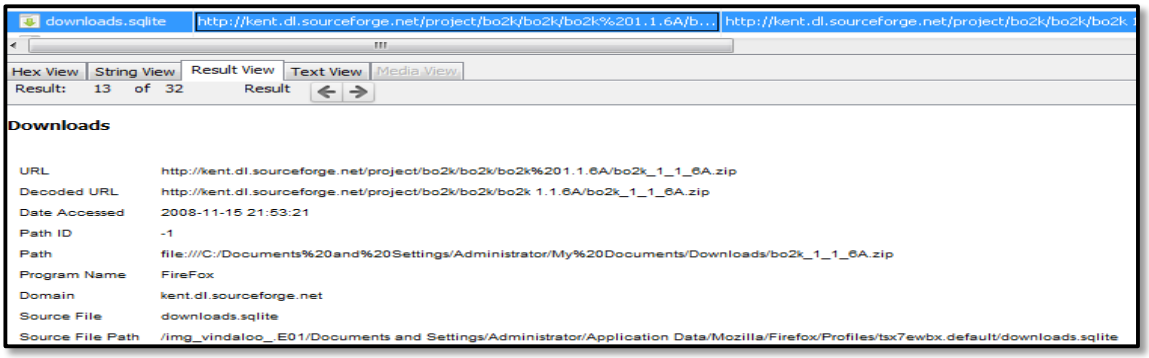


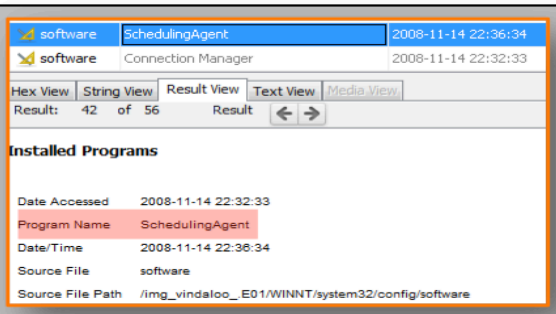
Figure 50. Entries of Bo2k found on "downloads.sqlite"

A.4.2.5 Evidence Item 9

Executable File – Evidence Item: SchedulingAgent: SchedulingAgent had been downloaded and installed in the 'Installed Programs' folder. Analysing this application, it appeared that it was a Backdoor Trojan. The full path is:

img_vindaloo_.E01/WINNT/system32/config/software

Table 14. Suspicious evidence item 9: executable file- SchedulingAgent

File Name:	**SchedulingAgent**	**File Hash**	**MD5: 6F39AC90AAAA1946315FBA63E8D0FED9 SHA1: 0F239FE18265FA6E4495E9757E90593903718DEB**
Evidence Item No:	N/A	Deleted?	No
Created Date:	Unclear	File Extension	OK
Modified Date:	14/11/2008 22:36:34	Duplicate	No
Accessed Date:	14/11/2008 22:32:33	L/P Size	9,003,008/ 9,003,008
Executable File:			

A.5 Steps Taken

A.5.1 Preserving Chain of Custody

On 2nd March 2016 at 13:00 PM, Detective Sergeant Huw Read provided the evidence item, 'hard drive image', which was in two segments including 'vindaloo_.E01' and 'vindaloo_.E02'. Both segments were in a folder entitled 'iy4s703'. The image had already been verified through matching **MD5 [4]** and **SHA1 [5]** checksums.

```
Image Verification Results:
 Verification started:  Mon Nov 30 17:01:15 2009
 Verification finished: Mon Nov 30 17:03:23 2009
 MD5 checksum:    66f8a508e95d7028e2a13bc8b044e761 : verified
 SHA1 checksum:   be90204aab3b74c402a760a48257ca782edc3b14 : verified
```

Figure 51. Log file of the original image

The hard drive image was held by the digital forensic analyst in his securely locked office for 70 days while all the forensic analysis was conducted, from 2nd March 2016 until 11th May 2016. At no time was the evidence was transferred to other individuals, nor were others able to interact with it. The evidence item was returned to Dr. Huw Read on 11th May 2016 at 09:00 AM.

A.5.2 Preparation for Digital Forensic Analysis

A.5.2.1 Forensic Analysis Workstation Specific Details

The followings are the details of the workstation through which the analysis was conducted:

- **Workstation:** Dell Desktop
- **Operating System:** Windows 7
- **System Type:** 32- bit Operating System
- **Processor [6]:** Genuine Intel(R) CPU
- **RAM [7]:** 2GB

The forensic analyst was the only user of this workstation with administrative rights: no others could access this machine and its resources. To secure the workstation and its resources, a secure password had also been set up to prevent unauthorised access. The workstation at all times was located in his office with a secure lock on the door.

A.5.2.2 Forensic Software Utilised

A wide range of legally approved and accepted forensic tools were utilised throughout the Exanimation and Analysis Processes. These included:

- AccessData FTK Imager 3.12 and FTK 4
- Autopsy 3.0.4
- Scalpel and Photerec Version 6.13
- LiveView
- VMware Player
- API monitors and rifiuti
- Virustotal (online malware checking tool)

A.5.2.3 Master Copy and Working Copy

Before starting the analysis, to maintain evidential integrity, two forensic sound copies of folder 'iy4s703' were made. The first, 'Master Copy', was a back-up made in case of corruption or damage. The second copied, '09031324-BOLtd-Vindaloo-Hacking', was the copy on which the Examination and Analysis Processes were conducted. The original copy folder 'iy4s703' was stored in a previously sterilized external hard drive in the investigator's secure office.

A.5.2.4 Image Verification

To maintain evidential integrity and ensure that the original hard drive image had not been modified, the image was again verified using FTK Imager 3.1.2.

MD5 Hash	
Computed hash	66f8a508e95d7028e2a13bc8b044e761
Stored verification hash	66f8a508e95d7028e2a13bc8b044e761
Report Hash	66f8a508e95d7028e2a13bc8b044e761
Verify result	Match
SHA1 Hash	
Computed hash	be90204aab3b74c402a760a48257ca782edc3b14
Stored verification hash	be90204aab3b74c402a760a48257ca782edc3b14
Report Hash	be90204aab3b74c402a760a48257ca782edc3b14
Verify result	Match

Figure 52. Original given HD image verified again through MD5 and SHA1 checksums

A.5.2.5 Converting Image to the Raw Format

The original image with 'EnCase-E01' file format was converted to a 'Raw' format to be able to interact with the image dynamically using 'LiveView' as well as being able to run 'data carving' on the image. Using FTK Imager 3.1.2, the copy of the original vindaloo image was first brought to the FTK Imager by adding it as an evidence item; and then to convert the image, the image was exported as a 'Raw' file. Using FTK imager 3.1.2, the 'Raw' image was verified through corresponding MD5 and SHA1 checksums.

```
MD5 checksum:     66f8a508e95d7028e2a13bc8b044e761
SHA1 checksum:    be90204aab3b74c402a760a48257ca782edc3b14

Image Information:
Acquisition started:   Wed Apr 03 18:32:50 2013
Acquisition finished:  Wed Apr 03 18:45:57 2013
Segment list:
 F:\University-MSc\AFDR\iy4s703\Vindaloo-Raw-Image\Vindaloo-Raw-Image.001

Image Verification Results:
Verification started:  Wed Apr 03 18:46:04 2013
Verification finished: Wed Apr 03 18:56:28 2013
MD5 checksum:     66f8a508e95d7028e2a13bc8b044e761 : verified
SHA1 checksum:    be90204aab3b74c402a760a48257ca782edc3b14 : verified
```

Figure 53. Raw image format verified through corresponding MD5 and SHA1 checksums

A.5.2.6 Case Creation

To analyse the hard drive image a case entitled *'09031324-BOLtd-Vindallo-Hacking'* was built within both software FTK 4 and Autopsy 3.0.4. For accuracy purposes and to ensure that the same results could be achieved by different forensic tools, two different analysis tools were used.

A.5.3 Digital Forensic Examination and Analysis

This section details the investigation methodologies and additional software deployed to carry out the examination and analysis of the hard drive image (working copy).

A.5.3.1 Virtualisation and API Monitor

VMware player running Windows XP guest was utilised to examine programs suspected of being malware in a 'controlled environment'. Using the 'snapshot' feature within the virtual machine allowed the restoration of the investigator's contaminated virtual machine. Moreover, API Monitors including 'Curprocess', 'Windump' and 'Kakeewar' were installed on the virtual machine to monitor the process of the suspicious programs. Below are the programs analysed and the findings:

Back Oriface

Before bringing Back Oriface to the virtual machine, a scan was run on the program using Avast local anti-virus. Avast marked the program as a Trojan and blocked it from running on the investigative machine. However, after bringing it to the VMware, the B2OK would not run, so it was not possible to monitor its process.

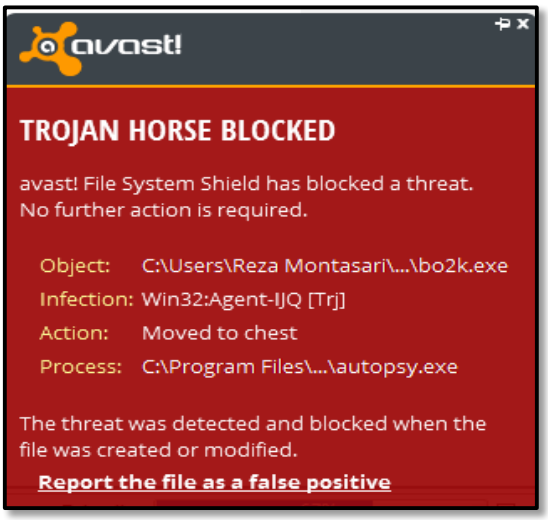


Figure 54. Avast anti-virus classifying B2OK as a Trojan program and blocking its opening

Dxdiag.exe

The 'dxdiag.exe' was examined inside VMware Player and found to be spyware, by interrogating the running process of the application via the installed API tools and finding the calls being made to the Guest Windows XP. The file path is: ***WINNT/system32/dllcache/dxdiag.exe***

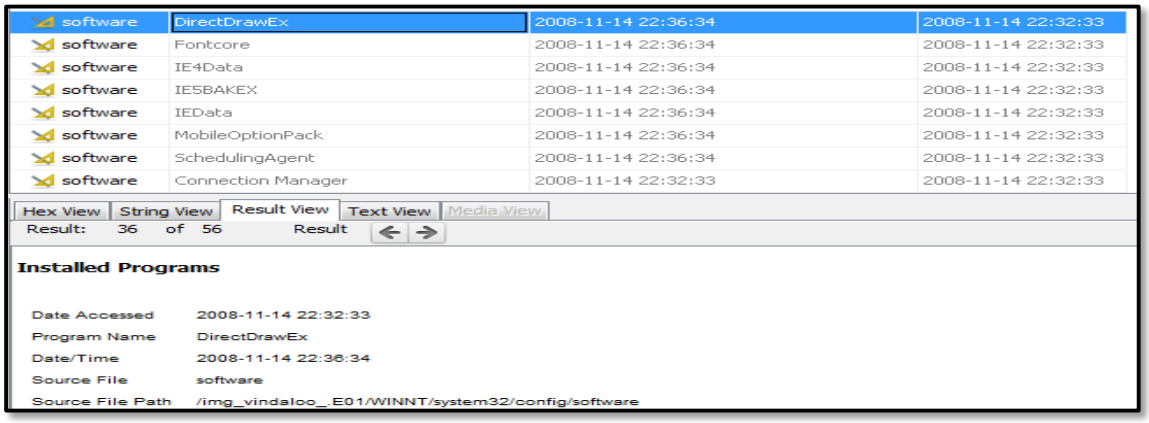


Figure 55. The 'dxdiag.exe' examined inside VMware Player and found to be spyware

A.5.3.2 Online Malware Checking Tool

'VirusTotal' was deployed to determine whether certain executable files were malware. To scan a suspicious executable file, the program was exported to the investigator's desktop and then, using 'VirusTotal', was browsed and scanned. For example, B2OK was scanned and marked as Trojan, with a quite high detection ratio of 21 out of 46.

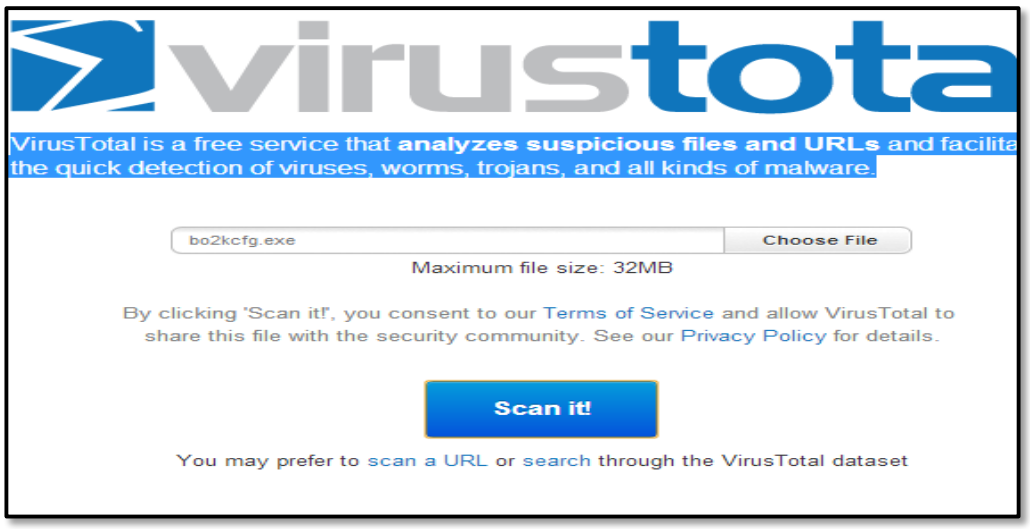
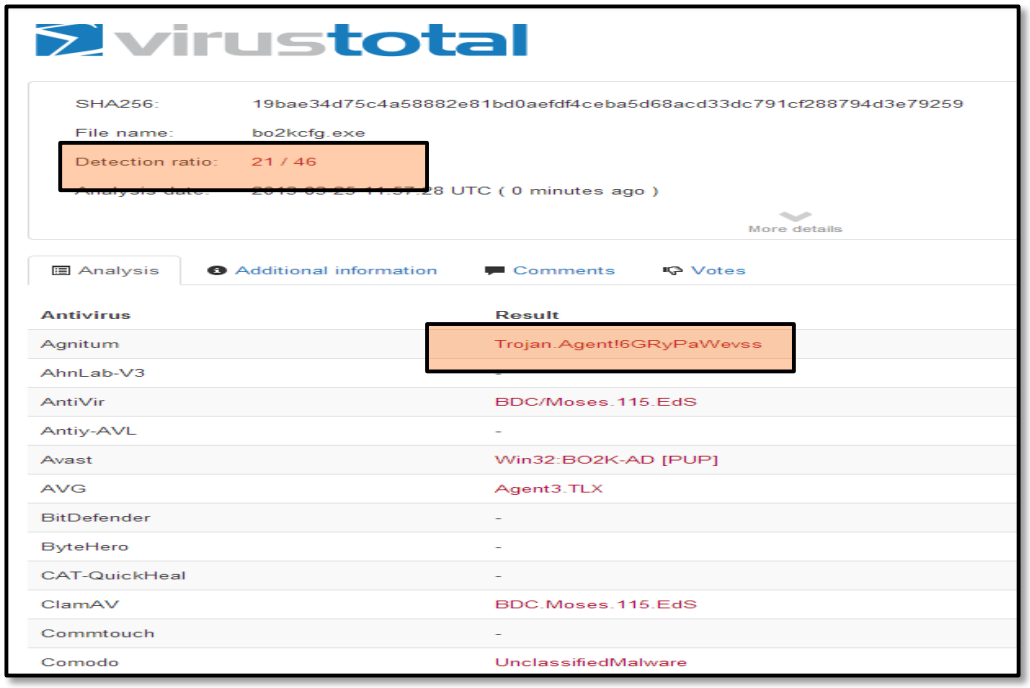


Figure 56. B2OK file browsed and scanned using VirusTotal



virustotal

SHA256: 19bae34d75c4a58882e81bd0aefdf4ceba5d68acd33dc791cf288794d3e79259
File name: bo2kcfg.exe
Detection ratio: 21 / 46
Analysis date: 2013-03-25 11:37:28 UTC (0 minutes ago)
More details

Analysis | Additional information | Comments | Votes

Antivirus	Result
Agnitum	Trojan.AgentI6GRyPaWevss
AhnLab-V3	-
AntiVir	BDC/Moses.115.EdS
Antiy-AVL	-
Avast	Win32:BO2K-AD [PUP]
AVG	Agent3.TLX
BitDefender	-
ByteHero	-
CAT-QuickHeal	-
ClamAV	BDC.Moses.115.EdS
Commtouch	-
Comodo	UnclassifiedMalware

Figure 57. The result of the scan showing B2OK as a Trojan program with high detection ratio

A.5.3.3 Live View

Live View was used to enable interaction with the image. To boot the image from Live View and mount it as a virtual hard drive, I firstly converted the provided image in 'E01' format to 'Raw' format (see A.5.2.5), then installed Live View with additional components including VMware Server and Java. This enabled me to examine the hard drive image as if I was the suspect browsing through the directories. Interacting with the 'Raw' image in Live View confirmed those items of evidence found from FTK 4 and Autopsy 3.0.4.

A.5.3.4 Recycler

Within the Recycler, MAC times were looked at. Times were in GMT and since the suspect was resident in South Wales, no conversion was necessary. The 'Recycler' contained 8 deleted files. All MAC activities regarding the deleted files happened between 15th and 26th November 2008.

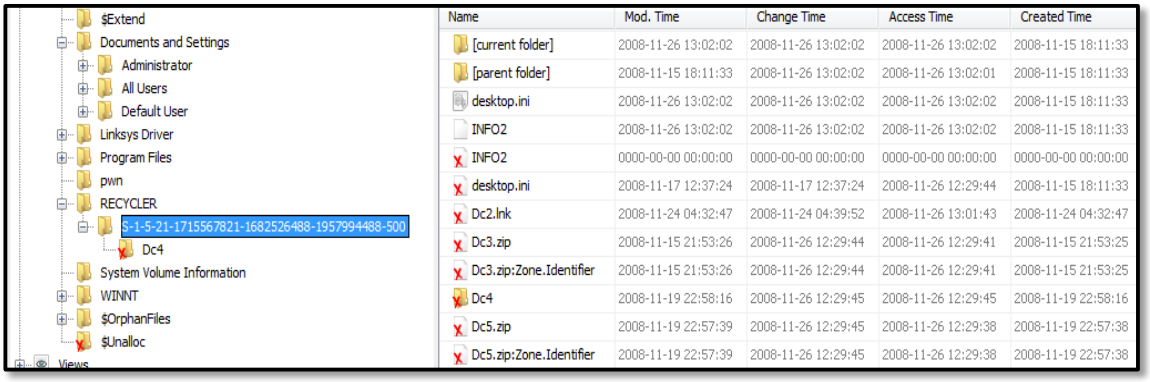


Figure 58. The deleted files in the recycler

Once placed in the 'Recycler', a file is renamed and retained until further instruction. As the above figure shows, the file names changed after the suspect moved them. Older versions of Windows OS assigned the format "DC#.XXX" to such files. 'DC' is the standard Windows given to deleted files, the numbers are the integer numbers allocated in the order files were received and 'XXX' is the original file extension. Although, as discussed in A.4.2.3, there was not enough evidence to prove that suspect had installed B2OK, this analysis confirms its deletion. The B2OK program, originally a zipped folder, was renamed 'DC3.zip' and placed in the 'Recycler' before the confiscation of the computer.

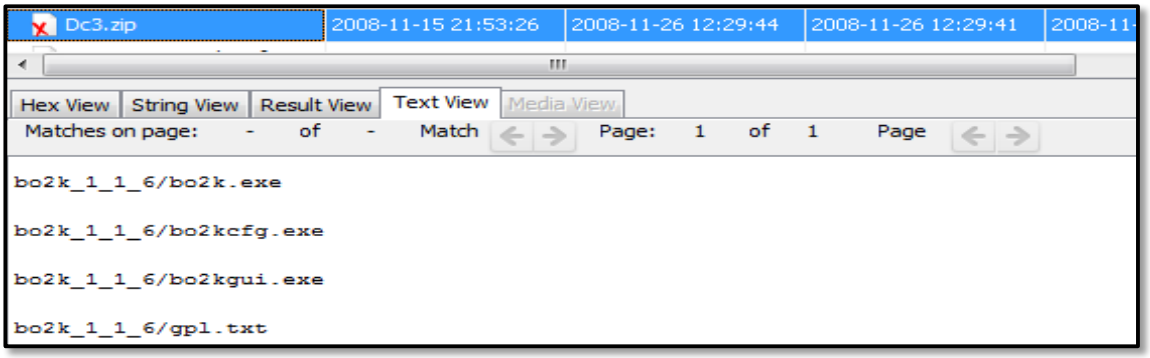


Figure 59. DC3.zip pointing to the previously downloaded B2OK program

However, given that the suspect had good IT skills, other files might have been permanently deleted by holding down the 'Shift Key' while deleting files to by-pass the 'Recycler' or by deleting them from the 'Recycler' directly. This required an analysis of whether any stored information concerning the assumed deleted files could be found in their original states. Being an old version of Windows OS, the 'Recycler' had a

master database holding all of the information entitled 'Info2' discussed in the next section.

A.5.3.5 rifiuti – INFO 2

Although a deleted file immediately appears in the 'Recycler', in the background the full path and file name are retained in a hidden file entitled 'Info2'. Two Info2 files were located, both pointing to the 'S-1-5-21-1715567821-1682526488-1957994488-500' folder placed in the 'Recycler'. The paths to these two files are:

/img_vindaloo_.E01/RECYCLER/S-1-5-21-1715567821-1682526488-1957994488-500/INFO2
/img_vindaloo_.E01/RECYCLER/S-1-5-21-1715567821-1682526488-1957994488-500/INFO2

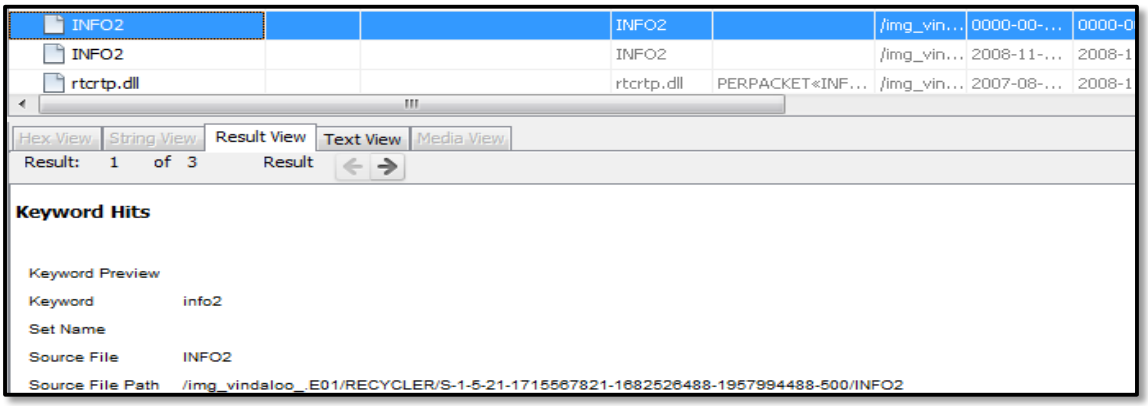


Figure 60. The paths to the INFO files: the INFO2 pointing to the "Recycler" deleted folder

A special tool 'rifiuti2' was then used to examine this INFO2. The INFO2, exported from FTK4, was copied to the 'rifiuti2' folder and the command 'rifiuti INFO2' was executed. No additional information was found.

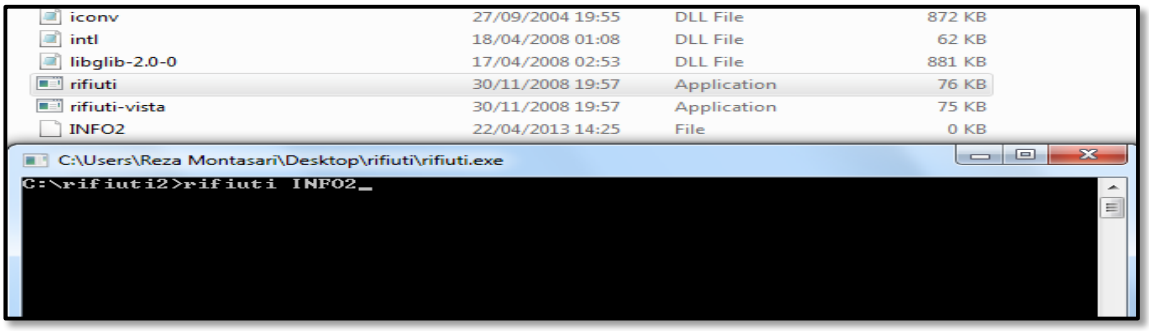


Figure 61. Analysis of "INFO2" in "rifiuti" revealing no further information

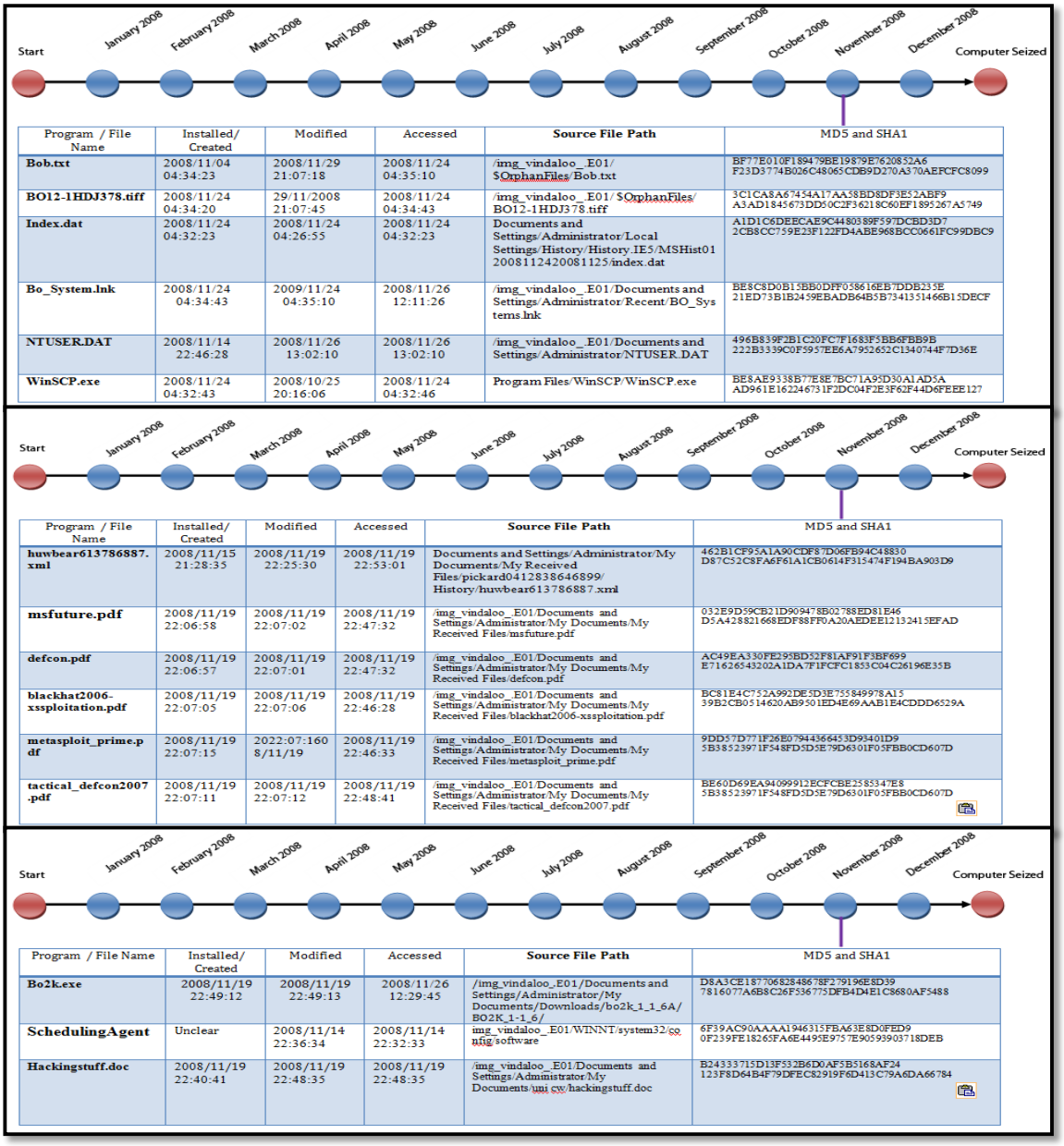
A.5.3.6 Search Function – Keyword Searches

The 'Search' function in FTK was frequently utilised to speed up the location of files which could be evidence items. As it was not clear where on the hard drive image certain files could be found, 'Index Search' was used more than 'Live Search' as it suggests similar hit results for search terms. Evidence items 4 'Bo_System.lnk' and 9 "hackingstuff" (sub-sections A.4.1.4 and A.4.2.2) were found through 'Index Search'.

A.6 Timeline of Important Events

Having conducted the Examination and Analysis Processes, I proceeded to create a concise timeline of important events associated with the case being investigated. This was to help to communicate this information more clearly. This section represents the timelines of various important events pertaining to the case. Due to the size of an A4 sheet, the timeline of a particular event might run through multiple figures.

A.6.1 Timeline of Items of Evidence



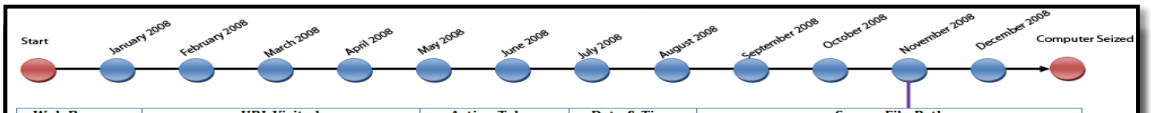
Program / File Name	Installed/ Created	Modified	Accessed	Source File Path	MD5 and SHA1
Bob.txt	2008/11/04 04:34:23	2008/11/29 21:07:18	2008/11/24 04:35:10	/img_vindaloo_.E01/ $OrphanFiles/Bob.txt	BF77E010F189479BE19879E7620852A6 F23D3774B026C48065CDB9D270A370AEFCFC8099
BO12-1HDJ378.tiff	2008/11/24 04:34:20	29/11/2008 21:07:45	2008/11/24 04:34:43	/img_vindaloo_.E01/ $OrphanFiles/ BO12-1HDJ378.tiff	3C1CA8A67454A17AA58BD8DF3E52ABF9 A3AD1845673DD50C2F36218C60EF1895267A5749
Index.dat	2008/11/24 04:32:23	2008/11/24 04:26:55	2008/11/24 04:32:23	Documents and Settings/Administrator/Local Settings/History/History.IE5/MSHist01 200811242008112 5/index.dat	A1D1C6DEECAE9C448 0389F597DCBD3D7 2CB8CC759E23F122FD4ABE968BCC0661FC99DBC9
Bo_System.lnk	2008/11/24 04:34:43	2009/11/24 04:35:10	2008/11/26 12:11:26	/img_vindaloo_.E01/Documents and Settings/Administrator/Recent/BO_Systems.lnk	BE8C8D0B15BB0DFF0 58616EB7DDB235E 21ED73B1B2459EBADB64B5B7341351466B15DECF
NTUSER.DAT	2008/11/14 22:46:28	2008/11/26 13:02:10	2008/11/26 13:02:10	/img_vindaloo_.E01/Documents and Settings/Administrator/NTUSER.DAT	496B839F2B1C20FC7F1683F5BB6FBB9B 222B3339C0F5957EE6A7952652C1340744F7D36E
WinSCP.exe	2008/11/24 04:32:43	2008/10/25 20:16:06	2008/11/24 04:32:46	Program Files/WinSCP/WinSCP.exe	BE8AE9338B77E8E7BC71A95D30A1AD5A AD961E162246731F2DC04F2E3F62F44D6FEEE127

Program / File Name	Installed/ Created	Modified	Accessed	Source File Path	MD5 and SHA1
huwbear613786887.xml	2008/11/15 21:28:35	2008/11/19 22:25:30	2008/11/19 22:53:01	Documents and Settings/Administrator/My Documents/My Received Files/pickard0412838646899/ History/huwbear613786887.xml	462B1CF95A1A90CDF87D06FB94C48830 D87C52C8FA6F61A1CB0614F315474F194BA903D9
msfuture.pdf	2008/11/19 22:06:58	2008/11/19 22:07:02	2008/11/19 22:47:32	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/msfuture.pdf	032E9D59CB21D909478B02788ED81E46 D5A428821668EDF88F0A20AEDEE12132415EFAD
defcon.pdf	2008/11/19 22:06:57	2008/11/19 22:07:01	2008/11/19 22:47:32	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/defcon.pdf	AC49EA330FE295BD52F81AF91F3BF699 E71626543202A1DA7F1FCFC1853C04C26196E35B
blackhat2006-xssploitation.pdf	2008/11/19 22:07:05	2008/11/19 22:07:06	2008/11/19 22:46:28	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/blackhat2006-xssploitation.pdf	BC81E4C752A992DE5D3E755849978A15 39B2CB0514620AB9501ED4E69AAB1E4CDDD6529A
metasploit_prime.pdf	2008/11/19 22:07:15	2022:07:160 8/11/19	2008/11/19 22:46:33	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/metasploit_prime.pdf	9DD57D771F26E07944366453D93401D9 5B38523971F548FD5D5E79D6301F05FBB0CD607D
tactical_defcon2007.pdf	2008/11/19 22:07:11	2008/11/19 22:07:12	2008/11/19 22:48:41	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/My Received Files/tactical_defcon2007.pdf	BE60D69EA94099912ECFCBE2585347E8 5B38523971F548FD5D5E79D6301F05FBB0CD607D

Program / File Name	Installed/ Created	Modified	Accessed	Source File Path	MD5 and SHA1
Bo2k.exe	2008/11/19 22:49:12	2008/11/19 22:49:13	2008/11/26 12:29:45	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/Downloads/bo2k_1_1_6A/ BO2K_1-1_6/	D8A3CE1877068284867 8F279196E8D39 7816077A6B8C26F536775DFB4D4E1C8680AF5488
SchedulingAgent	Unclear	2008/11/14 22:36:34	2008/11/14 22:32:33	img_vindaloo_.E01/WINNT/system32/config/software	6F39AC90AAAA1946315FBA63E8D0FED9 0F239FE18265FA6E4495E9757E9059390371 8DEB
Hackingstuff.doc	2008/11/19 22:40:41	2008/11/19 22:48:35	2008/11/19 22:48:35	/img_vindaloo_.E01/Documents and Settings/Administrator/My Documents/uni cw/hackingstuff.doc	B24333715D13F532B6D0AF5B5168AF24 123F8D64B4F79DFEC82919F6D413C79A6DA66784

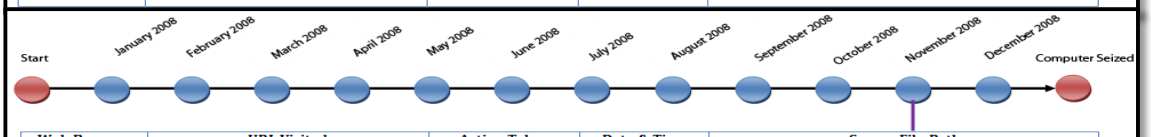
Figure 62. Timeline of items of evidence

A.6.2 Timeline of Web History and Downloads



Web Browser Used	URL Visited	Action Taken	Date & Time Accessed	Source File Path
Firefox	www.google.co.uk	Google Web Search Engine Queries ***bo***	2008-11-15 21:18:15	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***bo computers***	2008-11-15 21:21:52	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***bo computers***	2008-11-15 21:21:56	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***back oriface***	2008-11-15 21:23:46	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***bo2k***	2008-11-15 21:50:27	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	http://www.bo2k.com/	Visiting ***bo2k*** website	2008-11-15 21:50:31	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite

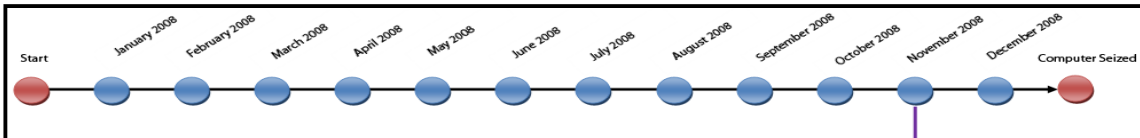
Web Browser Used	URL Visited	Action Taken	Date & Time Accessed	Source File Path
Firefox	http://www.bo2k.com/whatis.html	Finding out about ***b2ok***	2008-11-15 21:50:35	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	http://kent.dl.sourceforge.net/project/bo2k/bo2k/bo2k%201.1.6A/bo2k_1_1_6A.zip	Download b2ok	2008-11-15 21:53:21	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***essay for hacking***	2008-11-19 22:41:49	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	http://garr.dl.sourceforge.net/project/winscp/WinSCP/4.2.4%20beta/winscp424setup.exe	Download ***WinSCP***	2008-11-19 22:55:24	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***b02k source forge***	2008-11-19 22:55:54	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***b02k sourceforge***	2008-11-19 22:56:17	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite



Web Browser Used	URL Visited	Action Taken	Date & Time Accessed	Source File Path
Firefox	http://www.google.co.uk/search?client=firefox-a&rls=org.mozilla:en-GB:official&channel=s&hl=en&source=hp&q=essay trojan&meta=&btnG=Google Search	Google Web Search Engine Queries ***Essay Trojan***	2008-11-19 23:05:00	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	http://www.essaytown.com/topics/trojan_horse_essays_papers.html	Following his search term and visiting ***"essaytwon.com"***	2008-11-19 23:05:32	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite
Firefox	www.google.co.uk	Google Web Search Engine Queries ***winscp***	2008-11-24 04:29:25	Documents and Settings/Administrator/Application Data/Mozilla/Firefox/Profiles/tsx7ewbx.default/places.sqlite

Figure 63. Timeline of web history and downloads

A.6.3 Timeline of Installed Programs



Program Name	Date and Time Installed	Date and Time Last Accessed	Source File Path
WinSCP 4.2.4 Beta	2008-11-14 - 22:32:33	2008-11-24 - 04:32:47	WINNT/system32/config/software
MSN Messenger 7.0	2008-11-14 - 22:35:33	2008-11-15 20:50:26	WINNT/system32/config/software
SchedulingAgent	2008-11-14 22:32:33	2008-11-14 22:36:34	WINNT/system32/config/software

Figure 64. Timeline of installed programs

A.7 Conclusions

It appears that the suspect did penetrate the company's network, as the discovered Evidence Items 1 (email saved as a text file) and 2 (design of Circuit Boards) were confidential documents belonging to BOLtd, and he would have had to penetrate the network to acquire them. I do not regard as valid the potential counter-argument that a certain type of Trojan could have penetrated the network security and placed them on the suspect's system indirectly. There are two reasons to support the conclusion that the items of evidence were directly and consciously placed on the suspect's machine. Firstly, after identifying different types of Trojans on the suspect's system, using different tools such as Virtualisation, API monitors, Anti-Virus and an online tool, they were analysed. There was no evidence of any Trojan able to carry out such a penetration. Secondly, suspicious evidence items were found suggesting that the user was actively and consciously attempting to learn how to hack into a network. For example, he browsed and bookmarked questionable websites detailing network penetration techniques. The web browsing history further confirms nefarious intent. For example, there are several conversations with a friend through Windows Live Messenger, with discussions about possible methods of network hacking. The suspect's friend then sent five PDF files containing similar information. Similarly, based on a recovered word document appearing to be an assignment concerning hacking methods, the suspect seemed to have extensively researched the subject, acquiring knowing of network penetration techniques. Based on the findings, it appears that the suspect had used WinSCP to transfer unauthorised files from BOLtd Company. The forensic analysis of the hard drive image was repeated to ensure that the same results could be achieved for accuracy purposes. Someone studying a course in network security or computer forensics could have used his knowledge to destroy or hide other evidence items not recovered in this investigation. It may be that such an individual overlooked the deletion of the incriminating items of evidence that were found, or was too pressed for time to be able to delete them all.

Declaration: In arriving at the above conclusions, I made all the enquiries which I strongly felt were appropriate. I can testify that no matters of significance which I deem relevant have been withheld from the panel.

Appendix A1. Glossary of Terms

[1] PC Board: a thin board comprising of fibreglass and including electrical wires which connect the central processor to other components.

[2] Hard Drive Image: a complete copy of the hard drive contents.

[3] Back Orifice: a tool allowing system administrators to control a computer from a remote location.

[4] MD5: an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input that is claimed to be as unique to that specific data as a fingerprint is to an individual.

[5] SHA1: a SHA-1 sum is a calculation done on a file that produces a unique result. It is used to ensure the file hasn't been tampered with.

[6] Processor: the computer's brain, which tells the computer what to do and when.

[7] RAM: providing space for a computer to read and write data to be accessed by the CPU, RAM is volatile, so data stored stays there only whilst the computer is running.

[8] Data Carving: a method to recover deleted files.

[9] Index.dat: hidden files within a computer containing traces of websites visited.

[10] Log File: It keeps record of all of the a particular server's activities.

Appendix A2. Case Documents

Table 15. Evidence record document

UOG Lab Reference Number:	210413-RM01
Other Party Reference Number:	Dr. Huw Read and MR. Gareth Davis D:\hr_cw3\vindaloo_:
HD Image Description:	D:\hr_cw3\vindaloo_.E01 D:\hr_cw3\vindaloo_.E02
Additional Information:	Hard drive image which was handed in for analysis was into two segments in a folder titled iy4s703_cw; the folder contained a log file showing the HD image had been verified
Accepted on behalf of UoG by:	Reza Montasari
Signed in :	Reza Montasari
Delivered by:	Dr. Huw Read and MR. Gareth Davis
Signed in :	
Date and Time:	26/04/2016 at 11:10 AM
Returned on behalf of UoG by:	Reza Montasari
Signed out :	Reza Montasari
Delivered to:	Dr. Huw Read and MR. Gareth Davis
Signed out :	
Date and Time:	02/05/2016 at 09:00 AM

Table 16. Hard drive image document

Hard Drive Image "Vindaloo_.E01"		**Case Ref. No.**	210216-RM01
Exhibit. Ref. No.	RM- 21/02/2016	**No. Segments:**	2
Format:	E01	**Model:**	N/A
Serial No:	N/A	**Size:**	19077 MB
Cylinders:	N/A	**Heads:**	N/A
Sectors:	39,070,016	**Images:**	1 image into two segments
Imaging			
Method:	Created By AccessData® FTK® Imager 2.6.1.62 090803- Using 'Raw' File Format. The image, however, however was handed in a compact format (E01). Instructing party DR. Huw Read had laredy carried out the image verification through MD5 and SHA1 checksum values. The values are as follow: MD5 checksum: 66f8a508e95d7028e2a13bc8b044e761 : verified SHA1 checksum: be90204aab3b74c402a760a48257ca782edc3b14 : verified However, the image was once again verified by Reza Montasari, the forensic investigator, to ensure that no modification had been made to the image. AccessData ® FTK® Imager 3.1.8 was deployed for this purpose. The below are the matching MD5 and SHA1 values: MD5 checksum: 66f8a508e95d7028e2a13bc8b044e761 : verified SHA1 checksum: be90204aab3b74c402a760a48257ca782edc3b14 : verified		
Notes:	The Integral USB Drive has been found in the pocket of a known drug addict. A suspected drug dealer has been seen giving this USB drive to people whom he meets.		
Imaged By:	Instructing Parties DR. Huw Read MR. Gareth Davis	**Date and Time:**	Acquisition Started: Mon Nov 30 16:53:39 2009 Acquisition finished: Mon Nov 30 17:01:15 2009

Table 17. Job request document

UoG Reference Number:	210213-RM01
Other Party Reference Number:	Dr. Huw Read and MR. Gareth Davis D:\hr_cw3\vindaloo_:
Description of work to be carried out: Carrying out the analysis on the hard drive image of the suspect's computer to identify and recover any evidence items which could be related to the breach of network security of the BOLtd Company; the confiscated computer has been used to attack and penetrate the BOLtd's network security.	
Required date of completion:	02nd of May 2016
Accepted by:	Reza Montasari
Signed:	

Appendix B. Final Version of the Proposed Model

B.1 The CDFIPM's Abstract Representation

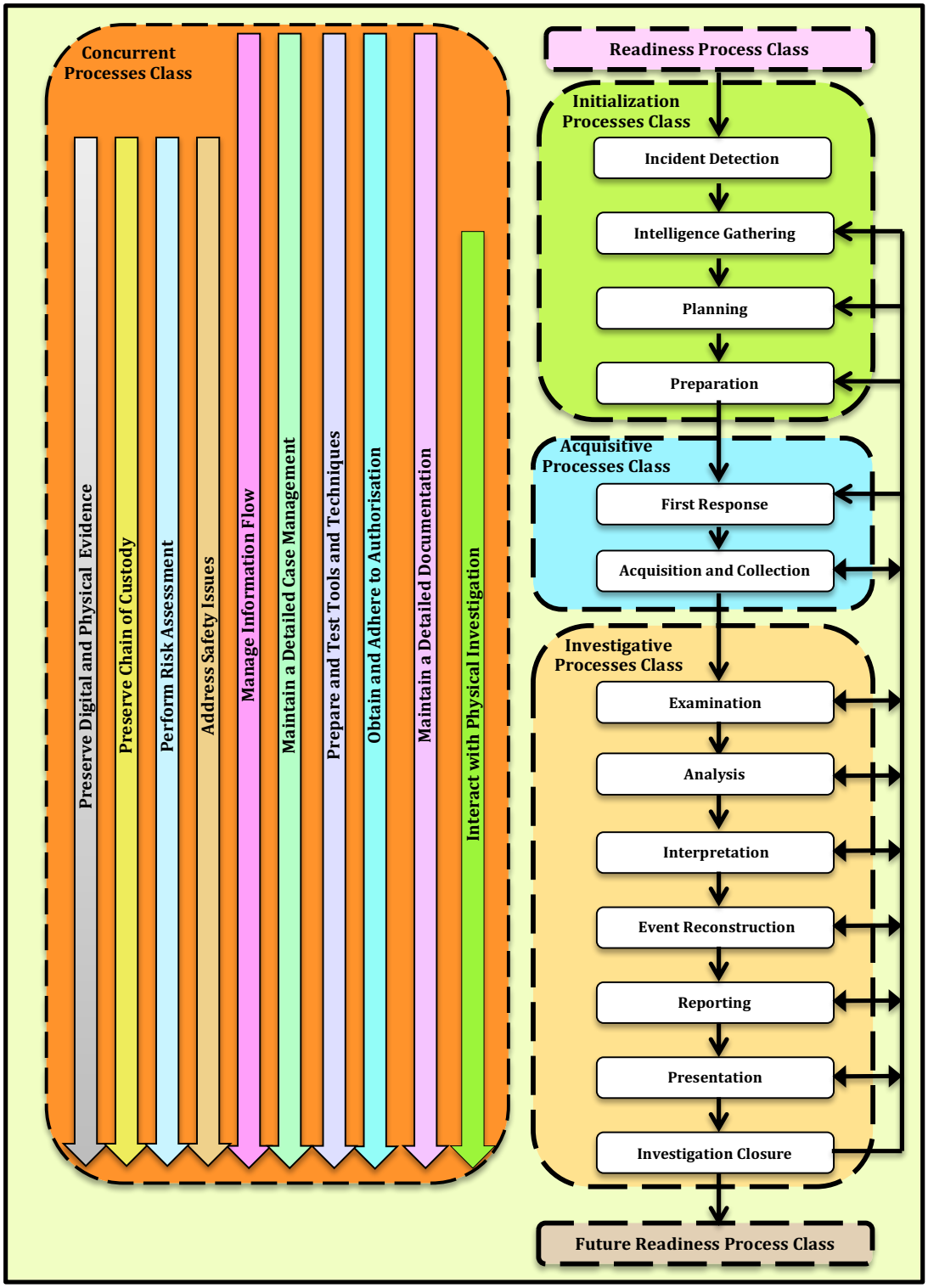


Figure 65. Final version of the CDFIPM's abstract representation

B.2 The CDFIPM's UML Activity Diagrams

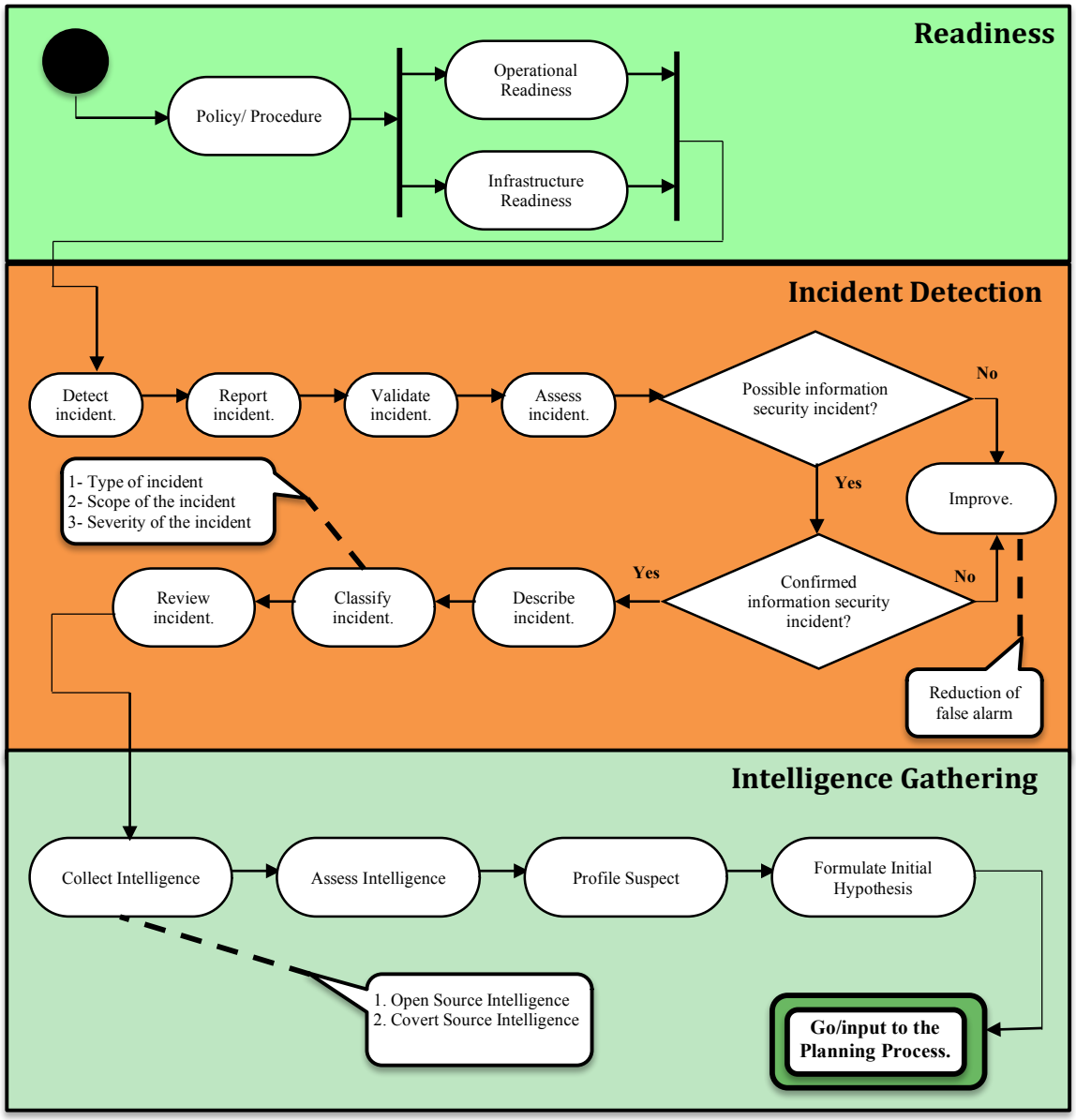


Figure 66. Final version of the Readiness, Incident Detection and Intelligence Gathering Processes

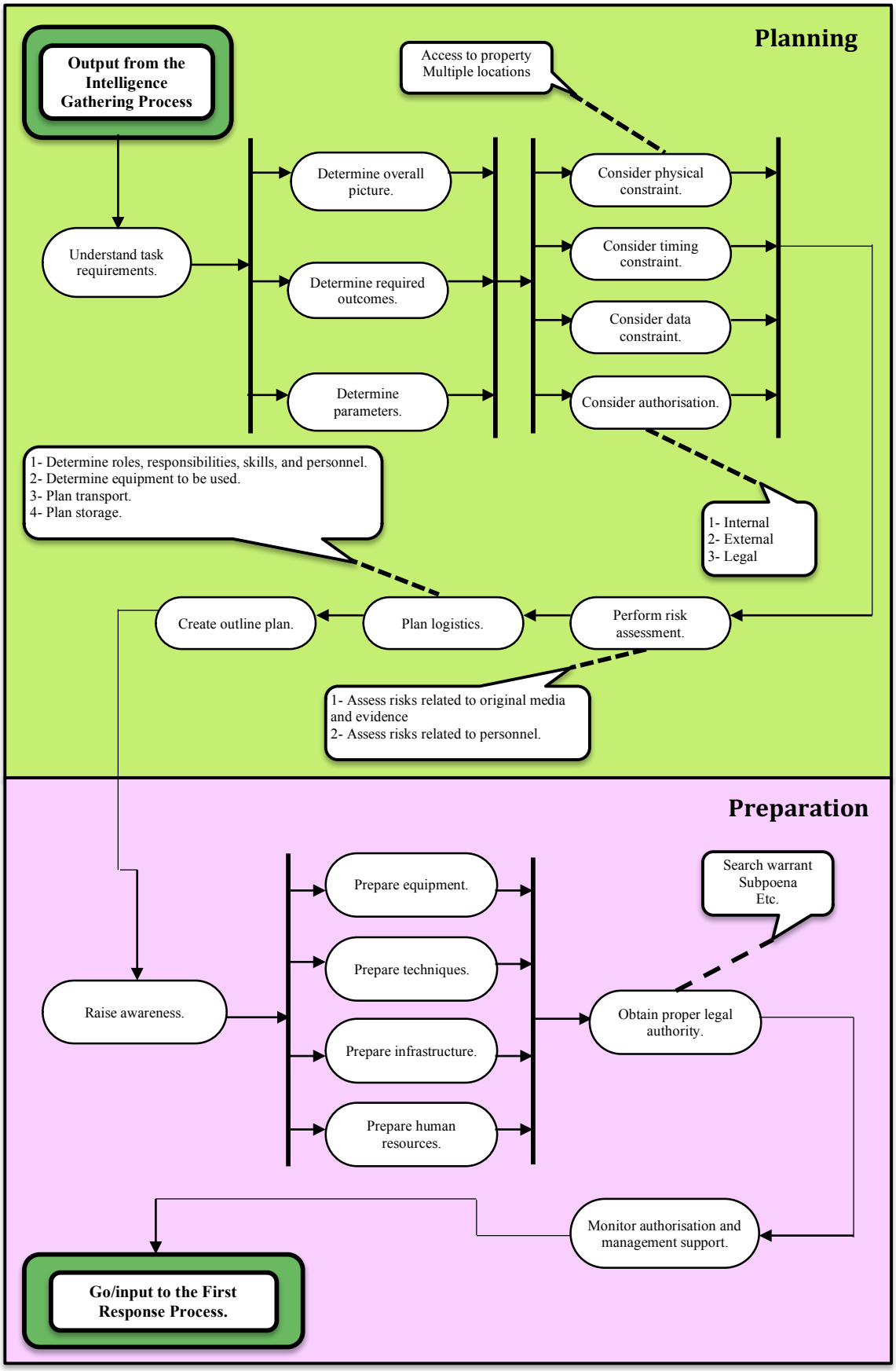


Figure 67. Final version of the Planning and Preparation Processes

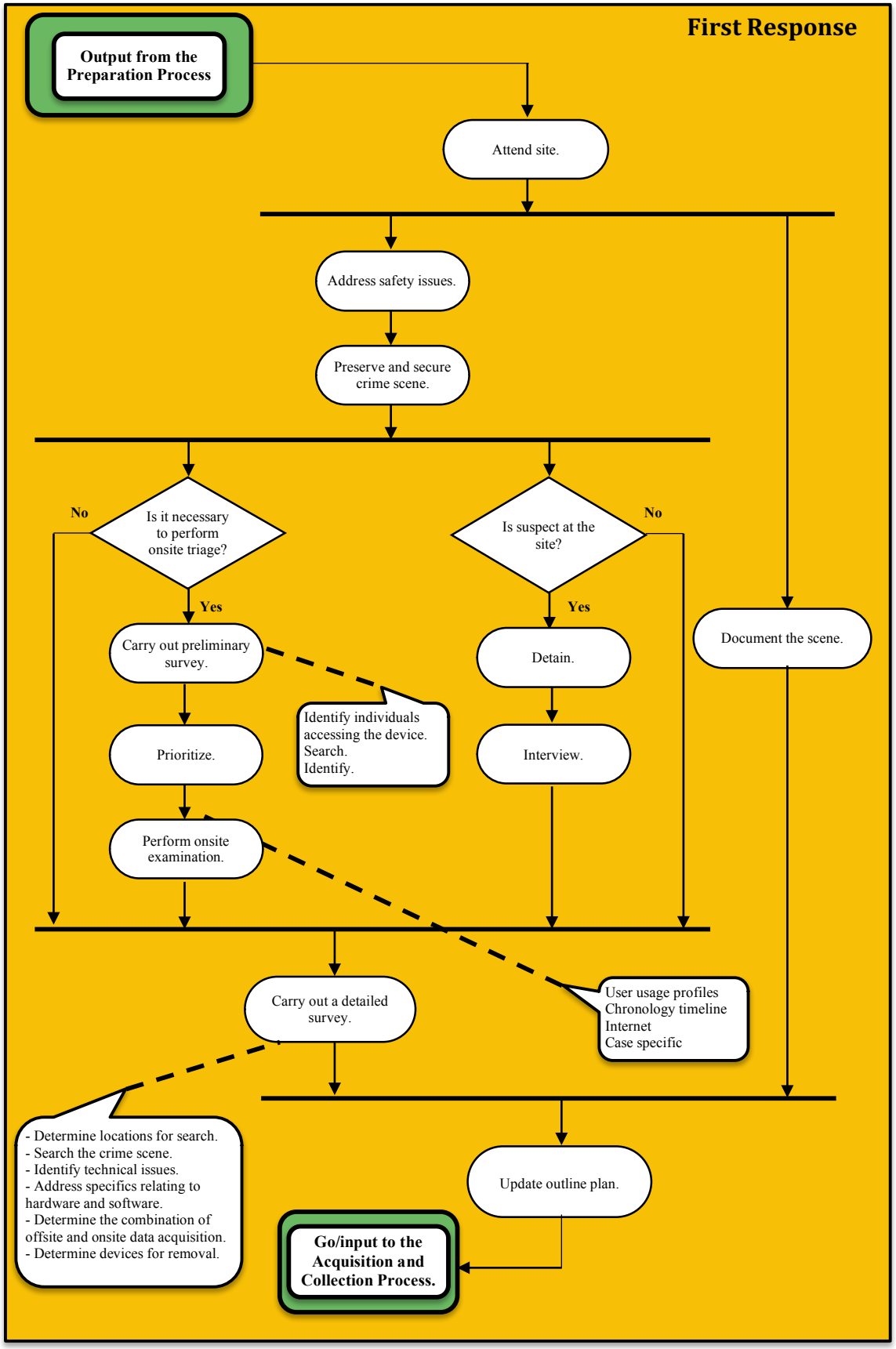


Figure 68. Final version of the First Response Process

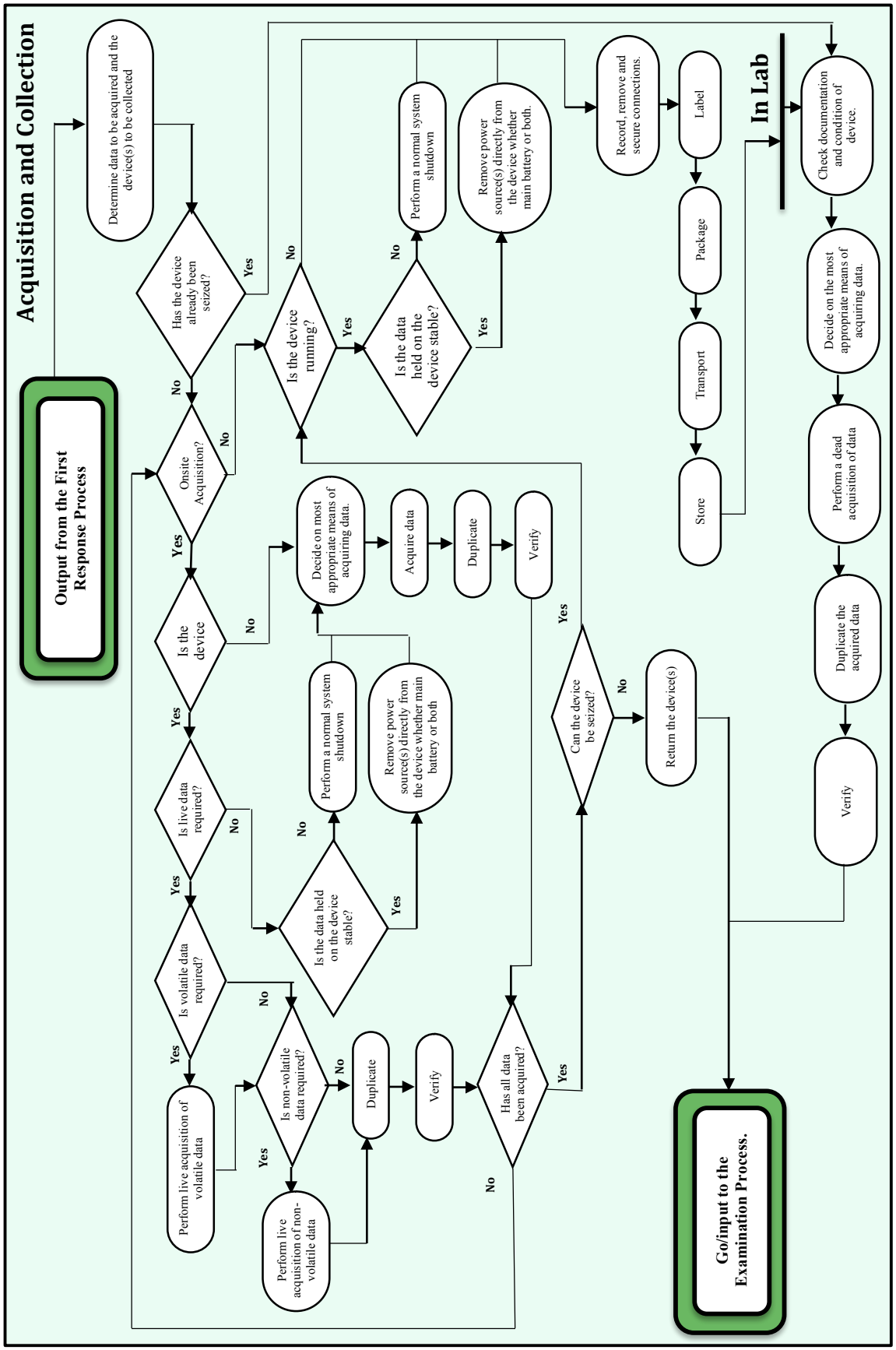


Figure 69. Final version of the Acquisition and Collection Process

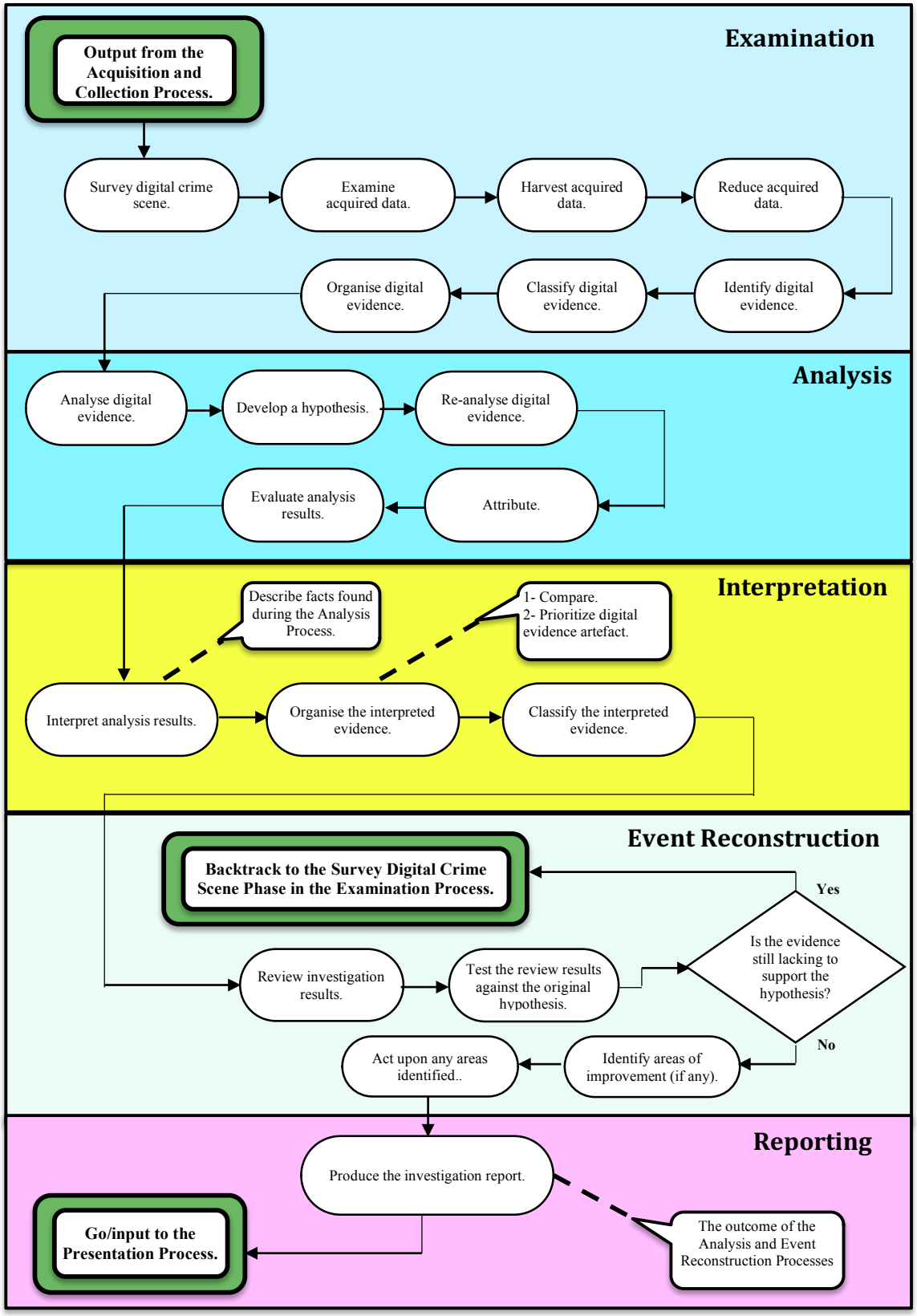


Figure 70. Final version of the Examination, Analysis, Interpretation, Event Reconstruction and Reporting Processes

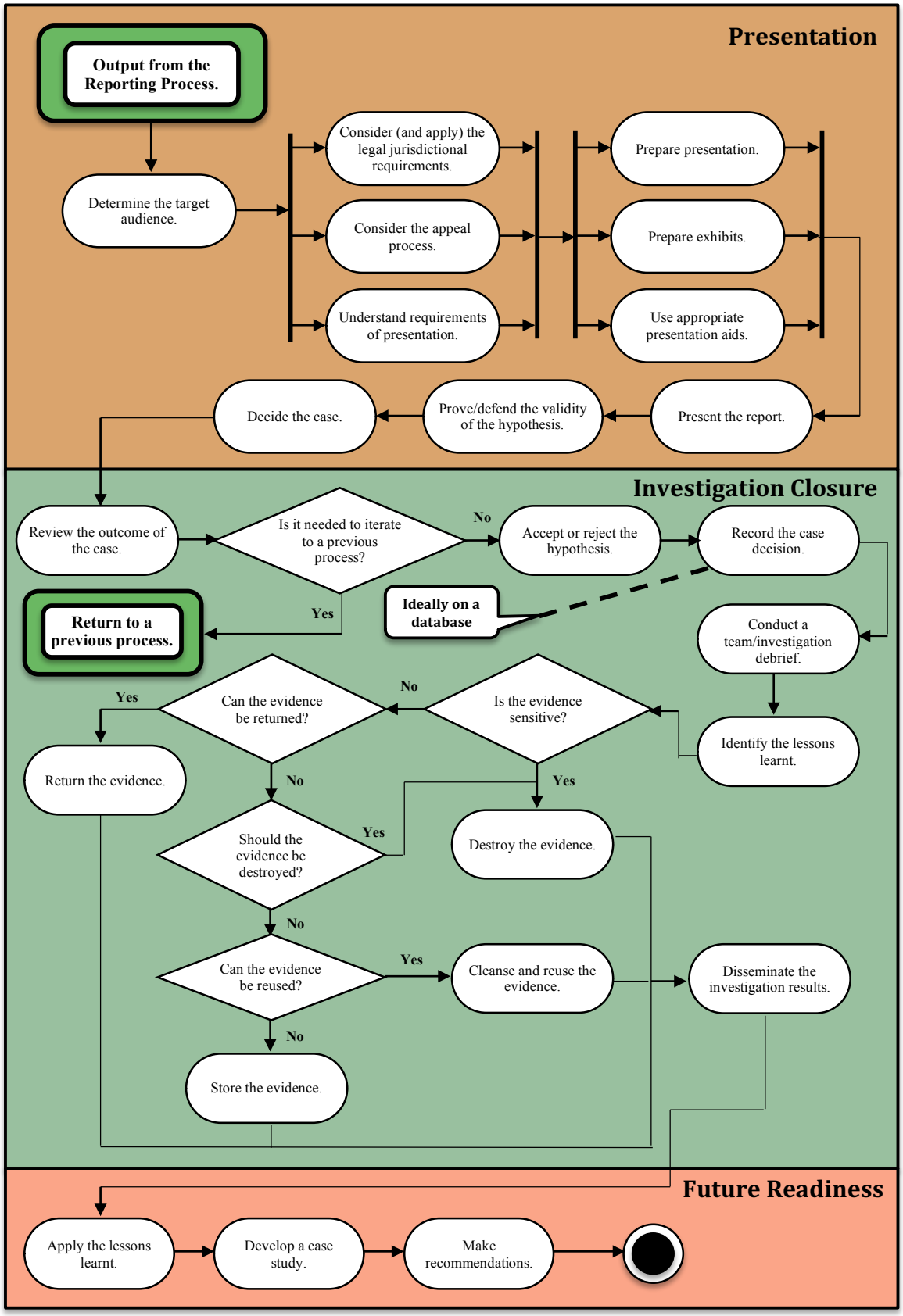


Figure 71. Final version of the Presentation, Investigation Closure and Future Readiness Processes