

A Comprehensive and Harmonised Digital Forensic Investigation Process Model

by

Aleksandar Valjarevic

A Comprehensive and Harmonised Digital Forensic Investigation Process Model

by

Aleksandar Valjarevic

THESIS

submitted in fulfilment of the requirements for the degree

DOCTOR OF PHILOSOPHY

in the subject

COMPUTER SCIENCE

in the

FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION
TECHNOLOGY

of the

UNIVERSITY OF PRETORIA

PROMOTER: PROFESSOR HEIN S. VENTER

ABSTRACT

Recent decades have seen a significant increase in the importance of the field of digital forensics as a result of the rapid development of information and communication technologies and their penetration into every corner of our lives and society. Furthermore, information security incidents are not only becoming more versatile every year, but are also growing in number, thus emphasising the importance of digital forensic investigations. Performing a digital forensic investigation requires a standardised and formalised process in order to ensure the admissibility of digital evidence, as well as the effectiveness and efficiency of investigations and collaboration between stakeholders. When this thesis was being prepared, there existed neither an international standard for formalising the overarching digital forensic investigation process, nor a process model that was accepted as a harmonised model across different jurisdictions worldwide.

The author studied existing state-of-the-art digital forensic investigation process (DFIP) models and concluded that there are significant disparities between them, pertaining to the number of processes, the scope, the hierarchical levels and concepts applied (for example, some of the models are based on the physical crime investigation processes, whereas others focus only on the digital aspects of the investigation process). This thesis proposes a comprehensive DFIP model that harmonises existing models for the purpose of establishing an international standard. An effort was made to incorporate all relevant types of processes proposed by the existing models, including those aimed at achieving digital forensic readiness, while introducing a number of novelties.

The author introduces a novel class of processes called *concurrent processes*. This is a novel contribution that should, together with the rest of the model, enable more efficient and effective digital forensic investigations, while ensuring the admissibility of digital evidence.

The author also proposes a prototype that would guide the user through the implementation of a standardised and harmonised DFIP, and ultimately validate the use of a proper digital forensic investigation process.

Both the proposed model and the prototype were tested and evaluated, and the results of these evaluations are presented in the thesis. The proposed model and the prototype contribute significantly to the field of digital forensics. The author believes its application would render

benefits that range from the higher admissibility of digital evidence and more effective investigations to easier cross-border collaboration on international investigations, thus fulfilling the initial reasons for creating a harmonised model. The proposed model is intended to be used for different types of digital forensic investigation and should ultimately culminate in an international standard. In fact, while this thesis was being written, an international standard on digital forensic investigation process model – as developed by the author was published as a result of the research reported on in this thesis.

Keywords: forensic science, digital forensics, investigation, process, model, harmonisation, standardisation, prototype

ACKNOWLEDGEMENTS

I dedicate this thesis to my beloved wife, Dragana Valjarevic, and my son Vukasin. They have never stopped showering me with enormous amounts of love, support and encouragement.

The completion of this thesis and subsequent PhD has been a long journey. At the end of this journey I wish to give a special word of thanks to several people without whose support I could not have succeeded:

- My parents, Zorica and Djurdje Valjarevic, and my brother Ljubisa, for their love and guidance, for instilling positive values in me, and for affording me a good education (Mama, tata, veliki brate, hvala Vam!);
- My promoter, Professor Hein S. Venter, for his guidance, encouragement, support and patience. It has been an honour and privilege to be your PhD student. Your patience and immense knowledge served as my constant motivation;
- My fellow student Ms Melissa Ingles, for her contribution to the software development and evaluation of the proposed prototype;
- My fellow students Ms Stacey Omeleze and Mr Emilio Mumba, for their contribution to the testing and evaluation of the proposed model;
- My friends Marko, Nikola and Stevan, for always being there for me and especially for believing in me;

- To my colleagues from Vlatacom d.o.o. and Vlatacom Research and Development Center, for their support throughout the years of my PhD studies. Special thanks to Mr Vladimir Cizelj, for motivating and supporting me, and to Mr Bosko Bozilovic for his mentorship and friendship;
- Anyone else who contributed to the completion of this research – I thank you all.

Contents

<i>Abstract</i>	ii
<i>Acknowledgements</i>	iv
PART 1: INTRODUCTION	1
CHAPTER 1- Introduction	2
1.1 Introduction to the subject of the thesis.....	2
1.2 Problem statement	3
1.3 Motivation for the study.....	5
1.4 Objectives.....	6
1.5 Layout of the thesis	7
PART 2: BACKGROUND	12
CHAPTER 2- Background on Digital Forensics and Related Work	13
2.1 Introduction.....	13
2.2 On digital forensics	13
2.3 On digital forensic readiness.....	15
2.4 Types of digital forensic investigations	16
2.5 Related work on digital forensic investigation process models	19
2.6 Related work on digital forensic readiness investigation processes	27
2.7 Conclusion	30
CHAPTER 3- Legal Aspects	31
3.1 Introduction.....	31
3.2 Legal aspects in relation to the digital forensic investigation process.....	31
3.3 Conclusion	34

PART 3: MODEL	35
CHAPTER 4- A Comprehensive and Harmonised Digital Forensic Investigation Process Model.....	36
4.1 Introduction.....	36
4.2 Methodology	36
4.3 A comprehensive and harmonised digital forensic investigation process model	37
4.4 Overview of the digital forensic investigation process classes	39
4.5 Readiness processes	41
4.5.1 Scenario definition	45
4.5.2 Identification of potential digital evidence sources.....	46
4.5.3 Planning pre-incident collection, storage and handling of data representing potential digital evidence.....	46
4.5.4 Planning pre-incident analysis of data representing potential digital evidence.....	47
4.5.5 Planning incident detection.....	47
4.5.6 Defining system architecture	47
4.5.7 Implementing system architecture	48
4.5.8 Implementing pre-incident collection, storage and handling of data representing potential digital evidence	48
4.5.9 Implementing pre-incident analysis of data representing potential digital evidence.....	49
4.5.10 Implementing incident detection	49
4.5.11 Assessment of implementation.....	50
4.5.12 Implementation of assessment results.....	50
4.6 Initialisation processes.....	50
4.6.1 Incident detection process	51
4.6.2 First response process.....	52

4.6.3	Planning process.....	52
4.6.4	Preparation process	53
4.7	Acquisitive processes	53
4.7.1	Potential digital evidence identification process	54
4.7.2	Potential digital evidence collection process.....	54
4.7.3	Potential digital evidence acquisition process	55
4.7.4	Potential digital evidence transportation process	56
4.7.5	Potential digital evidence storage process.....	56
4.8	Investigative processes.....	56
4.8.1	Potential digital evidence acquisition process	57
4.8.2	Digital evidence examination and analysis process.....	57
4.8.3	Digital evidence interpretation process.....	57
4.8.4	Reporting process.....	58
4.8.5	Presentation process	59
4.8.6	Investigation closure process	59
4.9	Concurrent processes.....	59
4.9.1	Obtaining authorisation	60
4.9.2	Documentation	60
4.9.3	Managing information flow	61
4.9.4	Preserving chain of custody	61
4.9.5	Preserving digital evidence.....	61
4.9.6	Interaction with the physical investigation.....	61
4.10	Digital forensic investigation process model schema	66
4.11	Conclusion	68
CHAPTER 5- Comparing Existing Models with the Harmonised Model		69

5.1	Introduction.....	69
5.2	Discussion of the comparison	69
5.3	Conclusion	83
CHAPTER 6- Analysis of the Results of Implementing the Proposed Process		
	Model.....	84
6.1	Introduction.....	84
6.2	Case 1 - Mobile digital forensic investigation into a case of intellectual property theft	85
6.2.1	Methodology	85
6.2.2	Case scenario	85
6.2.3	Details on the performed processes	86
6.2.4	Findings and observations.....	91
6.3	Case 2 - Mobile digital forensic investigation with regard to phishing using a scareware attack.....	95
6.3.1	Methodology	95
6.3.2	Case scenario	95
6.3.3	Findings and observations.....	96
6.4	Case 3 - Digital forensic post-mortem investigation with regard to the contravention of company user policy	97
6.4.1	Methodology	97
6.4.2	Case scenario	98
6.4.3	Findings and observations.....	98
6.5	Summary of the testing results	99
6.6	Conclusion	100
PART 4: PROTOTYPE		101
CHAPTER 7- Prototype for Guidance and Implementation of a Comprehensive and Harmonised Digital Forensic Investigation Process.....		
		102

7.1	Introduction.....	102
7.2	Prototype overview	102
7.3	Software development lifecycle.....	104
7.4	System architecture	104
7.5	Components	106
7.5.1	Reporting module.....	109
7.5.2	Process Implementation and Logging module	109
7.5.3	Guidance module	111
7.5.4	Digital signature verification module.....	113
7.5.5	Encryption module.....	114
7.6	Activity diagram for the main application	114
7.7	Functionality of the admin module of the prototype	117
7.7.1	User section.....	117
7.7.2	Organisation section	119
7.7.3	Project section	119
7.8	Information system security.....	122
7.9	Discussion on the proposed prototype	122
7.10	Conclusion	123
CHAPTER 8- Evaluation of the Proposed Prototype.....		124
8.1	Introduction.....	124
8.2	Usability testing results.....	124
8.3	Functional survey results	127
8.4	Discussion on the evaluation of the prototype.....	129
8.5	Conclusion	130

<i>PART 5: ISO/IEC 27043:2015 INTERNATIONAL STANDARD</i>	131
<i>CHAPTER 9- ISO/IEC 27043:2015 International Standard</i>	132
9.1 Introduction	132
9.2 About this international standard	132
9.3 Related standards	134
9.4 Comparison of ISO/IEC 27043:2015 international standard with related standards	139
9.5 Conclusion	145
<i>PART 6: CONCLUSION</i>	146
<i>CHAPTER 10- Critical Evaluation</i>	147
10.1 Introduction	147
10.2 Critical evaluation of the proposed model	147
10.3 Critical evaluation of the proposed prototype	151
10.4 Research questions	152
10.5 Conclusion	153
<i>CHAPTER 11- Conclusion</i>	155
11.1 Introduction	155
11.2 Revisiting the problem statement and research objectives	155
11.3 Thesis summary	156
11.4 Discussion on contributions and novelties	158
11.5 Future research work	159
11.6 Final conclusion	160
<i>References</i>	161
<i>Appendix A- List of Related Work Published by the Author</i>	172

<i>Appendix B- Terms and Definitions</i>	173
<i>Appendix C- List of Abbreviations</i>	178
<i>Appendix D- User Guide for a Prototype for the Guidance and Implementation of a Standardised Digital Forensic Investigation Process</i>	181
<i>Appendix E- Source Code for the Prototype for Guiding and Implementing a Standardised Digital Forensic Investigation Process</i>	197
<i>Appendix F– Electronic Copy of the Source Code for the Prototype for Guiding and Implementing a Standardised Digital Forensic Investigation Process</i>	199

List of Figures

Figure 1.1 Thesis layout.....	10
Figure 4.1 Classes of the proposed model	40
Figure 4.2 Readiness processes groups.....	42
Figure 4.3 Readiness processes.....	43
Figure 4.4 Initialisation processes.....	53
Figure 4.5 Acquisitive processes	55
Figure 4.6 Investigative processes	58
Figure 4.7 Comprehensive harmonised digital forensic investigation process.....	67
Figure 5.1 Comparing the proposed model with the existing models	82
Figure 7.1 Prototype Graphical User Interface	103
Figure 7.2 Basic interaction diagram	106
Figure 7.3 Details of the <i>reporting</i> module’s Graphical User Interface	109
Figure 7.4 Details of the <i>process implementation and logging</i> module’s Graphical User Interface.....	110
Figure 7.5 Details of the <i>guidance</i> module’s Graphical User Interface - textual advice.....	111
Figure 7.6 Details of the <i>guidance</i> module’s Graphical User Interface - graphical advice...	112
Figure 7.7 Details of the <i>guidance</i> module’s Graphical User Interface - graphical advice zoomed in	113
Figure 7.8 Activity diagram.....	115
Figure 7.9 Details of the <i>admin</i> module’s Graphical User Interface - user section	118
Figure 7.10 Details of the <i>admin</i> module’s Graphical User Interface - organisation section	120
Figure 7.11 Details of the <i>admin</i> module’s Graphical User Interface - project section	121
Figure 9.1 Applicability of standards to investigation process classes and activities [21]....	138
Figure 9.2 Comparing ISO 27043 and related international standards.....	142
Figure 9.3 Classes of standards according to width and depth	143

Figure 9.4 Classification of standards according to width and depth 144

List of Tables

Table 2.1 Sources of work used for benchmarking	26
Table 4.1 Overview of the digital forensics principles within related work models	65
Table 5.1 Comparison of existing models with the proposed harmonised model	70
Table 5.2 Comparison of the readiness processes class in the proposed model with readiness processes found in related work	75
Table 5.3 Number of processes present in the analysed models.....	78
Table 5.4 Characteristics of the analysed models	81
Table 6.1 Model evaluation table [72].....	93
Table 6.2 List of resources and equipment prepared for the investigation [75]	97
Table 7.1 Comparison of user roles	108
Table 8.1 Summary of SUMI results	125
Table 8.2 Summary of the functional survey results	128
Table 9.1 Characteristics of ISO 27043 and related standards	141

PART 1: INTRODUCTION

Part 1 of the thesis introduces the reader to the subject, defines the problem statement and objectives, explains the motivation for this study and provides a detailed layout of the thesis.

CHAPTER 1- INTRODUCTION

1.1 Introduction to the subject of the thesis

This section introduces the reader to the subject of this thesis through a discussion on the relevance and importance of digital forensics and digital forensics investigations in the modern world. Today, more than ever, one can say that we live in an information society – one in which the creation, distribution, diffusion, use, integration, and manipulation of information is a significant economic, political, and cultural activity [1]. We as humans and our societies are so dependent on information and on information technology that it is impossible to imagine life as it is without it. Information systems and information technology are everywhere, from smart phones in our pockets to complex systems managing traffic flows in cities and e-Government deployments. Information technology and information systems, and our interaction with these, are changing the ways in which we communicate, learn, work, build, conduct research, understand our environment and the way we govern our societies [2]. Therefore the security and availability of these information systems are very important issues.

At the same time, the number of information security incidents is constantly on the rise [3,4] and incidents are becoming more and more versatile [5]. They range from data leakages to attacks to information systems managing critical infrastructure such as power grids, and from random spam emails to targeted attacks with the aim to steal intellectual property from unsuspecting companies. Also, the cost of cyber-security incidents is ever increasing and is becoming a significant burden to economies [6, 7]. All of these further emphasise the importance of information systems security.

Information security incidents often require some form of digital forensic investigation, even if the incident does not represent a criminal act. The aim of such investigations is to set a hypothesis on how the incident occurred and who is to be held responsible, and then to prove the hypothesis. All of this confirms the importance of digital forensics as a tool to investigate digital evidence within information systems.

Digital forensics has gained importance rapidly over the past number of years due to the factors explained above.

The importance of digital forensics is evident from the fact that an entire forensic community existed by the time of writing of this thesis. For example, a digital forensics group on LinkedIn, called the Digital Forensic Association, has over 8200 members, with a year-on-year membership increase of about 70% [8]. Also, there are a significant number of national and international conferences that concentrate wholly or partially on digital forensics [9-15].

The importance of digital forensics is also clear from the large number of national and international bodies that are working towards the development and standardisation of this discipline, such as the European Network of Forensic Science Institutes (ENFSI) [16], the International Organization on Computer Evidence [17] and the International Federation for Information Processing Work Group 11.9 on Digital Forensics [18]. However, methods and especially process models for the digital forensic investigation process were – more often than not – developed mostly by practitioners and digital forensic investigators [19]. These models were usually based on personal experience and expertise, and on an ad hoc basis [19], without the main aim to achieve harmonisation and standardisation within in the field. Over the past decade, a number of academic research projects have also been conducted in order to establish a digital forensic investigation process model. The result is that there are still significant disparities between the different digital forensic investigation processes used, especially in different jurisdictions. Disparities range from scope and structure to concepts applied when process models were developed.

The next section defines and discusses the thesis problem statement. This statement is of crucial importance for the study presented in the thesis as it enables us to set the research questions and structure the research.

1.2 Problem statement

Dealing with digital evidence requires a standardised and formalised process in order for digital evidence to be accepted in a court of law. For example, consider the Daubert rule [20], which is most prominently used in the USA for expert witness testimony in criminal digital forensic investigation cases. The Daubert rule clearly states that theories and techniques used to draw conclusions in a case must result in positive answers to a number of questions, notably the question that asks whether the theories and techniques are subject to standards that govern their application.

When this thesis was being prepared, there existed neither an international standard for formalising the overarching digital forensic investigation process, nor a process model that was accepted as a harmonised model across different jurisdictions worldwide. Hence the author and a team of other researchers launched an effort to standardise and harmonise such a process within the International Standardization Organization (ISO) [21].

The existing digital forensic investigation process models are marked by significant disparities pertaining to the number of processes included, the scope of models and the scope of similarly named processes within different models, the hierarchy levels, and even concepts applied to the construction of the model (for example some of the models are based on the physical crime investigation processes). Disparities even exist in respect of the principles that must be observed or followed when conducting a digital forensic investigation.

Moreover, at present there exists no software application or a system that would guide one through all the components of a DFIP. Hence it is hard to properly implement a full DFIP and even harder to validate that a proper process was followed.

To conclude this section, the problem area identified can be split up into the following research questions:

1. Can we achieve comprehensiveness and harmonisation of the digital forensic investigation process?
2. Can we achieve standardisation of the digital forensic investigation process?
3. Can we propose a software application prototype that would guide one through the implementation of a comprehensive and harmonised digital forensic investigation process, while at the same time validating the use of a proper process?

The next section explains the motivation for this study. Such an explanation is of utmost importance as it shows what contributions the research should make and describes the desired effects of the research.

1.3 Motivation for the study

The need for a harmonised digital forensic investigation process model is most prominently experienced in a court of law. Being able to claim in court that a standardised set of processes was followed during a digital forensic investigation would render the cases concerned to be far less susceptible to any discrepancies within the investigation process followed. A number of court cases support this motivation. In *Trend Finance (Pty) Ltd and Another v Commissioner for the South African Revenue Service and Another* [22] in the Western Cape High Court, email printouts were rejected as digital evidence as proper process was not followed in order to be able to prove that the presented printouts present digital evidence (data messages). Another example is *State v. Dunn* [23] where the court concluded that “Admissibility of computer-generated records ‘should be determined on the basis of the reliability and accuracy of the process involved’”.

Furthermore, in the interconnected world of today there is a clear need for facilitating cross-jurisdictional and cross-border cooperation in digital forensic investigations and in the court proceedings of cases related to digital forensics. This fact was recently recognised and emphasised in the 2014 Internet Organised Crime Threat Assessment (iOCTA) document [24] prepared by the European Cybercrime Centre (EC3) at Europol. The strong need for cross-border collaboration was also identified at the recent Sixth International Forum on Cyber Security held in France. Thus the process of increasing cross-border and cross-jurisdictional cooperation in digital forensic investigations could be greatly assisted if a standardised DFIP model could be established.

Last but not least, this study is motivated by the need to provide better guidance for inexperienced professionals in the field and enable them to follow a harmonised DFIP.

The following section defines the specific objectives of the research. The objectives are based on the problem statement and provide concrete steps to be taken to solve the problem stated.

1.4 Objectives

The author defines the objectives of this study as follows:

- First objective – to introduce the reader to the subject matter and to study and analyse relevant existing digital forensic process models in order to make findings with regard to principles, harmonisation level and disparities.
- Second objective – to propose a digital forensic investigation process model that would comprise all benefits of existing state-of-the-art models and that would harmonise existing models. The proposed model should be comprehensive in terms of the individual processes included, especially digital forensic investigation readiness processes, which are often overlooked.
- Third objective – to compare the proposed model to existing models to verify comprehensiveness and achieved harmonisation.
- Fourth objective – to test the implementation of the proposed model to determine its usability, adaptiveness to different types of digital forensic investigation and its benefits and potential flaws.
- Fifth objective – to propose a prototype software application for the implementation of the proposed model. This application should help in providing guidelines and validating the use of the proposed process.
- Sixth objective – to ultimately expedite the standardisation of digital forensic investigation process.

The next section describes the detailed layout of the thesis. The author considered this explanation in the introductory chapter essential to enable the reader from the outset to fully understand the structure and contents of the thesis.

1.5 Layout of the thesis

This section gives an overview of the layout of the thesis.

The thesis consists of ten chapters that are divided into six parts:

- **Part 1** – Introduction
- **Part 2** – Background
- **Part 3** – Model
- **Part 4** – Prototype
- **Part 5**- ISO/IEC 27043:2015 International Standard
- **Part 6** – Conclusion

Part 1 contains only one chapter, namely the introduction. This chapter introduces the reader to the subject, defines the problem statement and explains the motivation of the study. The chapter also sets the objectives of the study and finally, provides the layout of the thesis.

Background chapters are grouped in **Part 2** of the thesis and include background on the following: digital forensics; digital forensic readiness; related work on digital forensic investigation process models; legal aspects of the digital forensic investigation process. These background chapters provide the reader with an overview of the background to the thesis subject and also present related work. The latter is of great importance as it was used as a starting point for the harmonisation of the proposed digital forensic investigation process.

Part 3 concerns the proposed model and contains three chapters, the first of which presents the proposed comprehensive and harmonised digital forensic investigation process model. The second chapter of **Part 3** compares the existing state-of-the-art models with the proposed model to show the comprehensiveness, holistic approach and benefits of the proposed model. The final chapter presents the results of testing the proposed process model, which was tried out on real-world cases to evaluate its usability and effectiveness.

Part 4 concerns the prototype and contains two chapters. The first proposes a prototype for guidance and implementation of the model proposed in **Part 3**, while the second provides information on the usability evaluation of the proposed prototype. A survey was also undertaken to evaluate whether the prototype meets the goals proposed.

Part 5 gives an overview of the international standard ISO/IEC 27043:2015 on the digital forensic investigation process that was published early in 2015. The model proposed in this thesis has served as key input for this standard and represents its basis. Furthermore, **Part 5** explains related international standards and compares these.

Part 6 concludes the thesis and consists of two chapters. The first provides a critical evaluation of the thesis contribution and the author discusses the proposed process, the proposed prototype, as well as the real-world testing results of the process and prototype implementation. Further, the author analyses the extent to which the research problem has been solved and the specific contribution made by the thesis and the specific novelties introduced. The final chapter concludes the thesis and provides indications of future work.

What follows next is an overview of the organisation and contents of the individual chapters within the six parts of the thesis.

The current chapter provides an introduction to the research problem. The rest of the thesis is organised as shown in **Figure 1.1**, followed by a summary of the remaining chapters.

Some of the work presented in this thesis has already been published in conference proceedings and scientific journals as shown in **Appendix A**.

Chapter 2 provides the reader with the background on digital forensics and digital forensics investigation processes, including digital forensic investigation readiness processes. The author also gives an overview of different types of digital forensic investigation. The aim of this chapter is to familiarise the reader with the basics of digital forensics, digital forensic readiness and corresponding processes. **Chapter 2** also presents state-of-the-art digital forensics investigation and digital forensic investigation readiness process models. Process models presented are used as a starting point to achieve harmonisation and comprehensiveness of the proposed process model and are therefore explained in this chapter by concentrating on their structure, individual processes, principles and main characteristics.

Chapter 3 contains background on legal aspects pertaining to digital forensics. This aspect is of importance as it strengthens the motivation for the study and helps the reader to understand the need for a comprehensive and standardised digital forensic investigation process model.

In **Chapter 4** the author presents the proposed comprehensive and harmonised digital forensic investigation process model that addresses the problem as stated in the study. The process model that is proposed involves a huge stride towards harmonisation and standardisation in the field of digital forensic investigation processes. In order to abstract all processes on a higher level, all digital forensic investigation processes in the proposed model are categorised into the following digital forensic investigation process classes [21]: *readiness process*¹ class, *initialisation process* class, *acquisitive process* class, *investigative process* class and *concurrent process* class. The processes proposed are defined in terms of scope, functions and order. It should be noted that the proposed harmonised model includes the comprehensive class of *readiness processes*, specifically to ensure that a holistic approach towards the digital forensic investigation process is taken. The author also introduces a novel class of processes called *concurrent processes*, defined as the investigation processes that are running in conjunction with other processes. The concept of concurrent processes is a novel contribution that should facilitate more efficient and effective digital forensic investigations. The proposed process model is one of the main inputs for the creation of an international standard on the subject, namely ISO/IEC 27043:2015, Information technology – Security techniques – Incident investigation principles and processes [21].

Chapter 5 provides a comparison of the proposed model and existing models to better explain the proposed model's comprehensiveness and the harmonisation achieved. This chapter also shows, through comparison, all novelties introduced by the proposed process model.

Chapter 6 analyses the results of testing the proposed process model. The chapter draws conclusions and presents findings on the process model's usability and effectiveness.

¹ Henceforward, the process class names or process names from the proposed model will appear in italics to support better readability of the text.

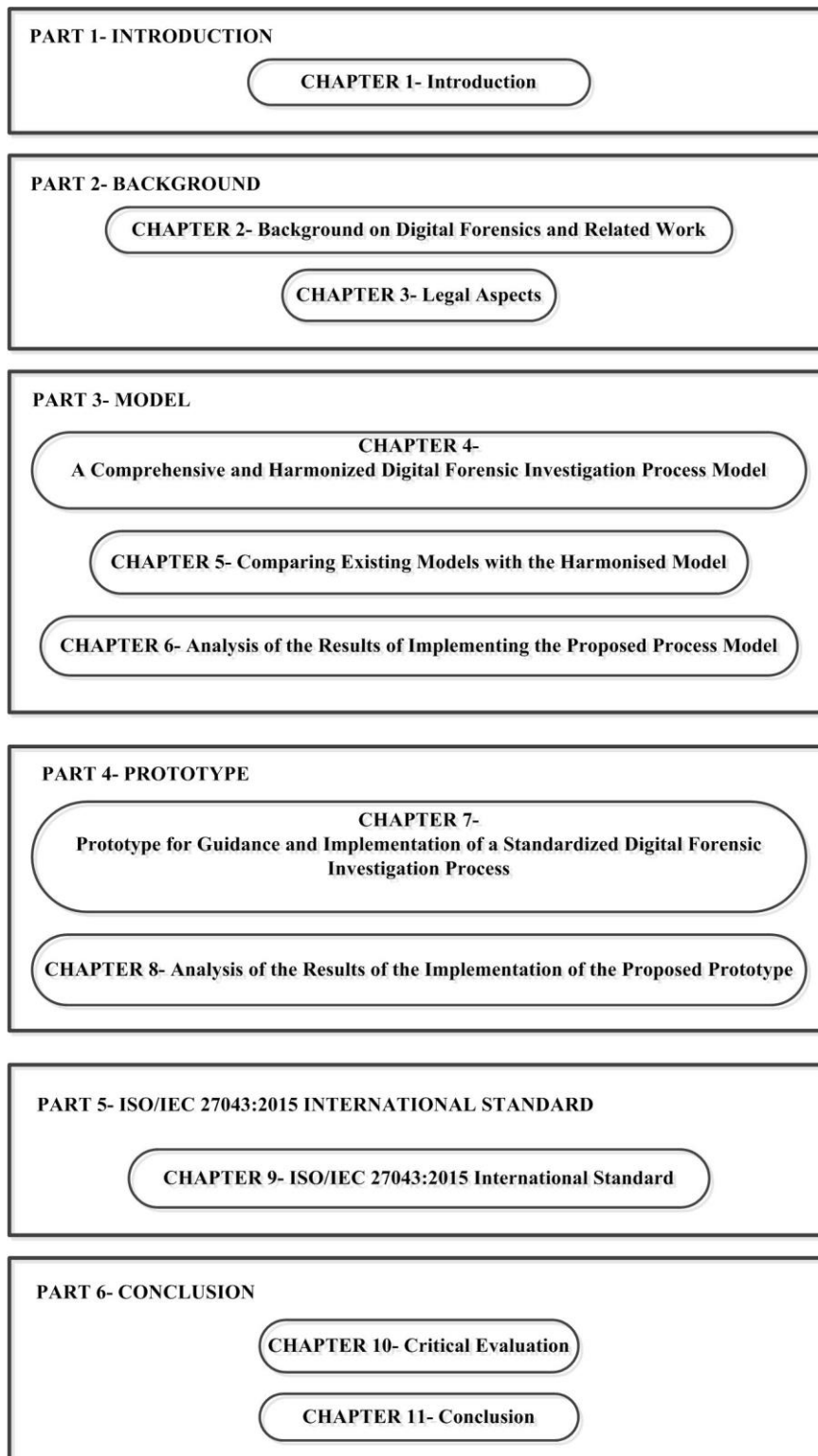


Figure 1.1 Thesis layout

In **Chapter 7**, the author proposes a prototype that guides one through the implementation of a standardised and harmonised digital forensic investigation process. The prototype is in the form of a software application that has two main functionalities, namely to act as an expert

system that can be used for guidance and training of novice investigators, and to enable the implementation of the investigation process while reliably logging all actions in a digital forensic fashion. Ultimately, the latter functionality would enable the validation of use of a proper digital forensic investigation process.

Chapter 8 analyses the results of usability and effectiveness testing of the proposed prototype. Conclusions on prototype effectiveness and usability are also presented in this chapter.

Chapter 9 is the only chapter in **Part 5** and it gives an overview of the international standard pertaining to the digital forensic investigation process. Through the author's engagement with the International Standardization Organization, the proposed digital forensic investigation process model represented the single main input to the creation of this international standard. **Chapter 9** also presents related international standards and compares these to the international standard on digital forensic investigation. The comparison is made to explain the role of the latter, as well as its uniqueness and comprehensiveness.

Chapter 10 provides a critical evaluation of the thesis contribution and concentrates on discussing the proposed process and the proposed prototype, as well as the real-world testing results of process and prototype implementation. Here, the author also analyses the extent to which the research problem has been solved. **Chapter 10** furthermore gives an overview of the significance of the research study presented in this thesis, including the importance of standardisation in the field of digital forensic investigation processes, the specific contribution of the thesis and specific novelties introduced.

Chapter 11 concludes the thesis and provides indications of future work.

Finally, a list of references is given, followed by appendices and an overview of terms and definitions.

Next follows **Part 2** of the thesis, which provides the relevant background information that is important for understanding the research, the research contribution and the research results.

PART 2: BACKGROUND

This part consists of two background chapters. The first presents background on digital forensics, digital forensic readiness and different types of digital forensic investigation. It also includes a review of related work on digital forensic investigation process models. The second chapter of **Part 2** gives an overview of relevant legal issues.

CHAPTER 2- BACKGROUND ON DIGITAL FORENSICS AND RELATED WORK

2.1 Introduction

The two sections to follow provide background on two main topics. First, a background on digital forensics is provided to introduce the reader to the definition of digital forensics and the basics of digital forensics. Next, background is provided on digital forensic readiness. The aim of these two sections of the chapter is to provide the reader with a basic overview and the most important aspects of digital forensics and digital forensic readiness.

The third section of **Chapter 2** outlines the different types of digital forensic investigation with a view to familiarising the reader with the versatility of the field. It is also important to understand the basics of these different types as the model that is proposed in this thesis is envisaged to accommodate all types of digital forensic investigation.

The last two sections of **Chapter 2** give an overview of state-of-the-art digital forensic investigation process models and digital forensic investigation readiness process models respectively. It is important to note here that the reason for the separate presentation of these two types of processes is because other authors have (more often than not) developed separate process models for digital forensic investigations and for digital forensic investigation readiness – an approach that the author of the thesis believes is fundamentally flawed.

2.2 On digital forensics

As explained in introductory chapter, the field of digital forensics has gained significantly in importance over the past number of years, due to an ever-increasing dependency on information technology and the rise in the number of information security incidents and cybercrime.

In her research, Beebe [25] concludes that the importance of digital forensic investigations has increased significantly. She motivates this conclusion by the statement that, nowadays, digital forensic investigations are a crucial part of all types of investigation – criminal, civil, military and corporate, and that digital forensics has even penetrated the world of popular crime shows on television, where it features prominently.

Further, the importance of digital forensics is evident from the fact that a number of national and international bodies are dealing with the subject and its regulation and progress. Next follows an overview of selected international bodies in the field, which signifies the importance of the field.

The European Network of Forensic Science Institutes (ENFSI) [16] is a network of forensic institutions from European countries. ENFSI activities include [16] the following:

- Organising meetings and scientific seminars, collaborative studies and proficiency tests
- Advising relevant partners on forensic issues
- Publishing best practice manuals of forensic terms in several languages

The International Organization on Computer Evidence [17] is an organisation appointed by the G8 countries (Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States of America) to draw up international principles for the procedures relating to digital evidence, to ensure the harmonisation of methods and practices among nations, and to guarantee the ability to use digital evidence collected by one state in the courts of another state.

Another international body working in the field of digital forensics is the International Federation for Information Processing Work Group 11.9 on Digital Forensics [18]. Their main activities include organising annual conferences that are recognised in the community as events where advances in digital forensics are presented, and publishing conference proceedings in the form of the “Advances in Digital Forensics” publication.

A definition of digital forensic investigation has been assembled by the author in previous research conducted by him.

The digital forensic investigation process is defined as the use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation and distribution and/or return and/or destruction of digital evidence derived from digital sources, while obtaining proper authorisations for all activities, properly documenting all activities, interacting with the physical investigation, preserving the evidence and the chain of custody, for the purpose of facilitating or furthering the

reconstruction of events found to be incidents requiring a digital forensic investigation, whether of a criminal nature or not [26].

Digital forensics is in practice applied whenever it is needed to investigate digital evidence as result of an incident, no matter whether the incident is of a criminal nature or not. Although digital forensic investigations are most often conducted when there is criminal charge related to an incident, this is not a rule, and digital forensic investigations are not limited to criminal investigations. For example, a digital forensic investigation might be needed when an employer wants to investigate and determine with certainty the amount of network capacity used by an individual employee, or the type of internet traffic that the individual employee creates.

The above statements can be supported by other authors' work. For example, Tan [27] states that digital forensics is important for all incidents requiring investigation as defined by the policies of the information system owner.

Although practice shows that the requirement to firmly follow certain digital forensic process is stronger in cases that are expected to finish in a court of law, the author believes that the same principles should be applied to investigations that are and those that are not expected to produce digital evidence for a court of law (for example an internal company investigation).

Digital forensic readiness is an important part of the digital forensics field, and it is often overlooked. The author finds that it is of great importance to take a holistic view and include digital forensic readiness. Therefore, the next section explains the basics of digital forensic readiness and presents relevant definitions and basic postulates.

2.3 On digital forensic readiness

Digital forensic readiness is defined as the ability of an organisation to maximise its potential to use digital evidence, whilst minimising the costs of an investigation [27].

A forensic investigation of digital evidence is commonly employed as a post-event response, but there are many circumstances in which an organisation may benefit from an ability to prepare itself for a potential digital forensic investigation by gathering, preserving and

processing potential digital evidence, even before the event that requires an investigation actually occurs.

We can say that digital forensic investigation readiness enables an organisation to prepare itself to perform a digital forensic investigation in a more efficient and effective manner.

Benefits include, but are not limited to, higher admissibility of digital evidence in a court of law, better utilisation of resources, and achieving higher awareness regarding information systems security and digital forensics within the organisations.

The following section discusses the types of digital forensic investigation.

2.4 Types of digital forensic investigations

The field of digital forensic investigations has become very versatile due to developments in and the advancement of information technology. Nowadays digital forensic investigations are often categorised according to the following types [28-34]:

- Post-mortem (also referred to as “dead”) forensics [28]
- Live forensics [29]
- Network forensics [30]
- Cloud forensics [31, 32]
- Mobile forensics [30, 33]
- Database forensics [34]

The author now gives a brief definition of the above types of investigation.

Post-mortem digital forensics is defined as the process of conducting a digital forensic investigation on an unpowered device [28]. Post-mortem digital forensics is sometimes also referred to as dead or static forensics [28, 32]. This type of investigation usually involves physically collecting from the investigation scene any devices that represent potential sources of digital evidence. Prior to collection, the devices are being powered off and disconnected from the computer networks. Once collected, the devices are usually transported to a digital

forensics laboratory. When the equipment arrives at the laboratory, the potential digital evidence is acquired in a forensically sound manner, after which the investigation continues through the necessary analysis and interpretation processes.

Live forensics is defined as an investigation that involves the process of extracting system data before disconnecting the digital device's power source, in order to preserve memory and information that would be lost if using the post-mortem approach [29]. This type of investigation is often conducted in conjunction with the post-mortem investigation in a situation where a digital device is found powered on, and a live acquisition of the device memory needs to be done to capture volatile potential digital evidence. The importance of this type of investigation is evident from the famous cybercrime case [35] where the accused, Aaron Caffrey, was acquitted of charges. Although his computer was used to launch a DDOS (Distributed Denial of Service) attack on an information system of the busiest port in the United States, he was actually found not guilty. He used a so-called "Trojan horse defence" [36] and claimed that the attack had been executed by Trojan horse malware and therefore he was also a victim in this case. Since prosecution could not prove that there was no trace of Trojan software in the Random Access Memory (RAM) of the seized computer – because they did not perform a live forensics investigation – Caffrey was acquitted.

Network forensics deals with preserving and collecting digital evidence travelling over a connected digital environment [30]. The term was first defined as "the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents" [37]. Network forensics has been perceived as a very important type of digital forensics because these days, electronic devices, including Personal Computers (PCs), notebooks, tablets, mobile phones, etc., are connected to a computer network virtually constantly.

Cloud forensics can be defined as the application of digital forensics to a cloud computing environment [31]. As the latter represents a digital connected environment we can freely say that cloud forensics represent a sub-type of network forensics. The field has emerged after the rise of the "cloud" concept in recent years and due to the fact that traditional methods of digital forensic investigation often cannot be applied to a cloud computing environment. Sibiya [32] states that both live forensic and static (post-mortem) forensic approaches face challenges in the cloud. He then explains [32]: "The static forensic process involves, for

example, shutting down the system so that the hard disk can be cloned. This cannot be carried out in the cloud as a number of virtual machines share the same physical infrastructure. Live forensics, on the other hand, only involves taking snapshots of running virtual machines and crime scenes cannot be recreated as in the case of static forensics.”

Mobile device forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions, using accepted methods [33]. This type of digital forensics is gaining more and more importance each day as users transfer from traditional computer platforms (PC, notebook) to mobile computing platforms (mobile phones, smart phones, tablets, wearable technology devices, etc.).

Database forensics is a branch of digital forensic science that involves the forensic study of databases and their related metadata [34]. Databases have become an integral and crucial part of any information system. Furthermore, databases are often mission-critical and business processes depend on them. All of these emphasise the importance of database forensics. A database forensic investigation can include database-specific activities such as protecting the audit trail, investigating Entity Relation Diagrams (ERD), checking for triggers, and collecting transaction logs [38].

One can note from the definitions given above that these types of investigation are not mutually exclusive and that a digital forensic investigation can for example be mobile and live. Also, one digital forensic investigation can include different activities that would belong to different types of digital forensic investigation. For example, an investigation into a suspect who used a cloud computing platform to launch a phishing attack could potentially include all of the types of digital forensic investigation defined above (mobile forensics to investigate suspect’s cell phone, dead forensics to investigate his computer, live forensics to investigate his tablet and finally cloud, network and database forensics to investigate the cloud platform itself).

This strongly emphasises the need for a harmonised and comprehensive process model that would serve as “umbrella” model for all types of digital forensic investigation.

The following two sections give an overview of digital forensic investigation process models and digital forensic investigation readiness process models respectively. The focus is on the structure of the models, principles applied or prescribed, and individual processes included in

the process model. The author also analyses the similarities and disparities of presented models.

2.5 Related work on digital forensic investigation process models

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [39], the need for a standard framework for digital forensics has been widely acknowledged [40-46]. The digital forensic investigation process model proposed at this workshop includes the following seven processes:

1. Identification
2. Preservation
3. Collection
4. Examination
5. Analysis
6. Presentation
7. Decision

The process model was defined as iterative.

Reith et al. [40] proposed a digital forensic investigation process model known as the abstract model, which includes the following processes:

1. Identification
2. Preparation
3. Approach strategy
4. Preservation
5. Collection
6. Examination

7. Analysis
8. Presentation
9. Returning evidence

The US Department of Justice (DOJ) published a process model in the Electronic Crime Scene Investigation Guide for first responders [41]. This proposed process model includes the following processes:

1. Preparation
2. Recognition and identification
3. Documentation of the crime scene
4. Collection and preservation
5. Packaging and transportation
6. Examination
7. Analysis and reporting

Carrier and Spafford [42] propose a process model based on the following requirements that they identified:

- The model must be based on existing theory for physical crime investigations.
- The model must be practical and follow the same steps that an actual investigation would take.
- The model must be general with respect to technology and not be constrained to current products and procedures.
- The model must be specific enough to allow for the development of general technology requirements for each process.
- The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response.

The model proposed by Carrier and Spafford [43] includes 17 processes that are organised into the following five groups:

1. Readiness processes
2. Deployment processes
3. Physical crime scene investigation processes
4. Digital crime scene investigation processes
5. Review processes

It is important to note here that they introduced a model that is based on a physical crime investigation.

Mandia et al. [43] proposed a digital forensic investigation process known as the incident model, which contains the following processes:

1. Pre-incident preparation
2. Detection of the incident
3. Initial response
4. Response strategy formulation
5. Duplication (system backup)
6. Investigation
7. Secure measure implementation (isolation and containment of the suspect system)
8. Network monitoring
9. Recovery (recovery of the suspect system to original process)
10. Reporting and follow-up

Beebe and Clark [44] proposed a hierarchical, objectives-based digital forensic investigation process model and also drew a comprehensive comparison between their proposed process model and previous works in this field. The model they proposed is multi-tiered, which constitutes a novel approach. First-tier processes proposed in [44] include the following:

1. Preparation
2. Incident response
3. Data collection
4. Data analysis
5. Findings presentation
6. Closure

In their opinion, second-tier sub-processes should be defined in such a way that these are inclusive of all possible types of crime and types of digital evidence.

Cuardhuáin [45] proposed a very comprehensive model of cybercrime investigations that combined and generalised models existing at the time, while also extending the scope of the proposed model beyond that of existing models. His model included the following processes:

1. Awareness
2. Authorisation
3. Planning
4. Notification
5. Search for and identification of evidence
6. Collection of evidence
7. Transport of evidence
8. Storage of evidence

9. Examination of evidence
10. Hypothesis
11. Presentation of hypothesis
12. Proof/Defence of hypothesis
13. Dissemination of information

Very importantly, the model proposed by Cuardhuáin [45] also includes information flow description between different processes, an element that does not feature in previous models and hence represents a novelty.

According to Casey and Rose [46], the processes of the digital forensic investigation process can be defined as doing the following:

- Gathering information and making observations
- Forming a hypothesis to explain observations
- Evaluating the hypothesis
- Drawing conclusions and communicating findings

Cohen [47] proposed a process model that includes the following processes:

1. Identification
2. Collection
3. Preservation
4. Transportation
5. Storage
6. Analysis
7. Interpretation

8. Attribution
9. Reconstruction
10. Presentation
11. Destruction

In addition to their earlier model [42], Carrier and Spafford [48] also proposed another event-based process model. This model is again based on a physical crime investigation and it is suggested that a digital crime scene investigation should occur as a subset of a physical crime scene investigation. The work concentrates on digital crime scene investigation processes and how to find the causes and effects of events during a digital forensic investigation.

Cohen et al. [49] discuss the state of the science of digital evidence examination and consensus in digital evidence examination. They recognise that numerous calls have been made for scientific approaches and formal methods in the field of digital forensics.

In the United Kingdom, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence [50, 51]. These guidelines do not explicitly set out the digital forensic investigation process model, but through recommendations the process model can be constructed, containing the following processes:

1. Preparations for investigation
2. Crime scene group of processes
3. Securing and control of the crime scene
4. Photographing and documenting the scene
5. Initial collecting of volatile data
6. Attaching exhibit labels
7. Documenting each action performed

8. Transportation
9. Storage
10. Evidence recovery group of processes
11. The collection process
12. The examination process
13. The analysis process
14. The reporting process
15. Disclosure

What follows next is an analysis of the source type for the models that the author used as a benchmark and as a starting point for developing the proposed model.

The source types are divided into four categories, namely:

- Peer-reviewed journals
- Peer-refereed books or book chapters
- Technical reports
- Government -issued guidelines

As can be seen from the table below, the documents selected for benchmarking represent a combination of Government-published documents and state-of-the-art academic work in the field. All of these documents are the result of peer-reviewed work and represent high-quality work, when compared to for example conference papers and non-peer-reviewed conference papers, ad hoc work, etc.

Table 2.1 Sources of work used for benchmarking

Model	Peer-reviewed journals	Peer-refereed books or book chapters	Technical reports	Government-issued guidelines
Palmer [39]			X	
Reith et al. [40]	X			
DOJ [41]				X
Carrier and Spafford [42]	X			
Mandia et al. [43]		X		
Beebe and Clark [44]	X			
Cuardhuáin [45]	X			
Cohen [47]		X		
Casey and Rose [46]		X		
ACPO [51]				X

Based on related work on the digital forensic investigation process, the author of this thesis concludes that there are significant disparities among existing digital forensic investigation process models. Disparities pertain to the number of processes included, the scope of models, and the scope of similarly named processes within different models, the hierarchy levels and even concepts applied to the construction of the model (i.e. some of the models are based on the physical crime investigation processes). Other authors have also come to similar conclusions. In their work, Reith et al. [40] state that there is a lack in standardisation of digital forensic models. They argue that existing models have significant differences, due to the fact the existing models are often too technology specific and were developed without generalisation in mind.

Reith et al. [40] are of the opinion that there is a dearth of knowledge and peer-reviewed papers on the digital forensic investigation process and that experts and practitioners in the field should concentrate on researching and publishing more on this subject.

Another group of authors, namely Yusoff et al. [52], produced interesting work that further adds to showing the level of disparity between existing digital forensic process models. This disparity is clearly evident from the results of work by Yusoff et al. [52] who analysed 15 different digital forensic investigation models [39, 40, 42, 44, 45, 53-62] and identified a total of 46 different processes as part of these models. Furthermore, 30 of the processes identified by Yusoff et al. [52] are present in only one of the models analysed in his work and not in any of the remaining 14, which shows the full extent of the disparity between existing digital forensic investigation models. The disparity in this case is demonstrated by the fact that the same or similar processes are called different names in different models, that processes are often divided to create more processes, and that different models include different process groups (for example some include readiness processes and some not), thus resulting in the large number of processes appearing in only one of the models analysed in [52].

The author of this thesis has however initiated an effort to standardise the digital forensics process within the International Standardization Organization (ISO) [21]. This international standard provides guidelines that encapsulate idealised models for common investigation processes across various investigation scenarios [21]. The research reported on in this thesis presents an important input to the development of standard ISO/IEC 27043:2015 [21], which is intended to complement other standards and documents that provide guidance on the digital forensics investigation process.

The following section presents related work on digital forensic investigation readiness processes. In the author's opinion digital forensic investigation readiness process presents a core part of the digital forensic investigation process. However, more often than not, digital forensic investigation readiness processes were proposed as separate models from digital forensic investigation process models.

2.6 Related work on digital forensic readiness investigation processes

This section provides an overview of past work on digital forensics investigation readiness processes (DFIRP) and requirements and aims of digital forensic readiness.

As explained in **Chapter 2**, digital forensic readiness is defined as the ability of an organisation to maximise its potential to use digital evidence, whilst minimising the costs of an investigation [47].

What follows, is a brief overview of work related to the digital forensic readiness processes.

Tan [27] identified the following factors that affect digital forensic readiness:

- How logging is done
- What is logged
- Intrusion Detection Systems (IDSs)
- Digital forensic acquisition
- Digital evidence handling

Yasinac and Manzano [63] propose six categories of policies to facilitate digital forensic readiness:

1. Retaining information
2. Planning the response
3. Training
4. Accelerating the investigation
5. Preventing anonymous activities
6. Protecting the evidence

Wolfe-Wilson and Wolfe [64] emphasise the need for an organisation to have procedures in place to preserve digital evidence in the event that a digital forensic investigation (DFI) is needed.

Rowlingson [65] defines a number of goals for digital forensic readiness:

- To gather admissible evidence legally and without interfering with business processes
- To gather evidence targeting the potential crimes and disputes that may have an adverse impact on an organisation
- To allow an investigation to proceed at a cost in proportion to the incident

- To minimise interruption to the business from any investigation
- To ensure that evidence makes a positive impact on the outcome of any legal action

Rowlingson [65] also defines key activities in the implementation of digital forensic readiness:

- Defining the business scenarios that require digital evidence
- Identifying available sources and different types of potential evidence
- Determining the evidence collection requirement
- Establishing a capability for securely gathering legally admissible evidence to meet the requirement
- Establishing a policy for the secure storage and handling of potential evidence
- Ensuring monitoring is targeted to detect and deter major incidents
- Specifying circumstances when escalation to a full investigation should be launched
- Training staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence
- Documenting an evidence-based case describing the incident and its impact
- Ensuring legal review to facilitate action in response to the incident

As indicated in the previous section, there are also several works presenting digital forensic models that include readiness as a process, policy or principle, as discussed above. However, to the best knowledge of the author, no harmonised digital forensic investigation readiness process model is proposed. Existing related models are quite disparate in terms of scope and level of guidance provided.

The harmonised model proposed in this thesis includes the digital forensic investigation processes as an integrate part of the model.

The following section concludes this chapter.

2.7 Conclusion

In this chapter the author started by providing background on digital forensics and digital forensic readiness. He then analysed state-of-the-art digital forensic investigation process models and proposed digital forensic investigation readiness processes and activities. Significant disparities were found among the existing models and there was a clear need to achieve harmonisation in this field. Presented models were used as starting point for construction of the model proposed in this thesis.

The existing digital forensic investigation process models and associated guidelines, procedures and individual processes were mostly developed by practitioners in the field, based on the need to conform to a certain legislative environment. Legal aspects pertaining to the digital forensic investigation process are of importance if one is to understand the basic requirements of the process and understand the motivation to have a formalised, harmonised and ultimately standardised process. The relevant legal aspects are presented next, with a focus on legal requirements for a standardised process model.

CHAPTER 3- LEGAL ASPECTS

3.1 Introduction

In this chapter the author provides an overview of the legal aspects pertaining to digital forensics and especially the need to use standardised (recognised) processes to achieve the admissibility of digital evidence in a court of law.

This legal overview is not comprehensive but aims to provide the reader with a sense of the need for a harmonised, and ultimately, a standardised digital forensic investigation process.

3.2 Legal aspects in relation to the digital forensic investigation process

Legal requirements may differ extensively in different jurisdictions across the world. The premise of this section is not to advocate specific legal systems, but rather to note the generic requirements, rules and guidelines in terms of legal issues that can be adopted by the legal system in any jurisdiction.

In the United States of America cases that require the presentation of digital evidence are treated under rule 702 of the Federal Rules of Evidence [66], which says: "If scientific, technical, or other specialised knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise." For application of this rule, the Daubert rule [20] is the most important. In the Daubert case, the court suggested the following factors to be considered [20]:

- Whether the theories and techniques employed by the scientific expert have been tested
- Whether they have been subjected to peer review and publication
- Whether the techniques employed by the expert have a known error rate
- Whether they are subject to standards governing their application

- Whether the theories and techniques employed by the expert enjoy widespread acceptance

It is clear from the above that the use of a harmonised, widely accepted and ultimately standardised and tested digital forensic investigation process would benefit the digital forensic community at large and add to the higher probability of the acceptance of digital evidence and the results of digital forensic investigations in a court of law and in general.

Other countries have similar guidelines aimed at digital forensic investigations or parts of it [51, 67, 68].

As mentioned earlier, examiners in the United Kingdom, usually follow the guidelines issued by the Association of Chief Police Officers (ACPO) to authenticate and confirm the integrity of evidence [50, 51]. The Conference on the Admissibility of Electronic Evidence in Court (AEEC) provided an overview of the results of the AEEC project, which had been partly funded by the European Union. A number of those present at the conference expressed the view that it would be good to have a European-wide law on electronic evidence for criminal proceedings [67].

All of the above clearly indicates the need for one harmonised and standardised digital forensic process model.

As stated in the introductory chapter of this thesis (see **Section 1.3**), a number of court cases support this outlook. Reference was made to the case of Trend Finance (Pty) Ltd and Another v Commissioner for the South African Revenue Service and Another [22] in the Western Cape High Court, where email printouts were not accepted as digital evidence because proper process had not been followed to prove that the presented printouts established digital evidence (data messages). Namely, one of the parties in the court case presented what was claimed to be printouts of data messages, where data messages in fact represent digital evidence. However, no due process was followed while creating the printouts to ensure and prove that the printouts represent a copy of the actual data message. Further, the party did not present any proof in the form of a copy of the digital evidence itself (the actual data message in question). Because of these reasons, the court rejected the evidence.

Another example referred to in **Section 1.3** involves the case of *State v. Dunn* [23] in which the court concluded that the “admissibility of computer-generated records should be determined on the basis of the reliability and accuracy of the process involved”. The case involved computer-generated telephone records as proposed evidence. The accused appealed against the judgment convicting him of two counts of forcible rape, two counts of forcible sodomy, one count of first-degree burglary, one count of sexual abuse, and four counts of third-degree assault of an 85-year-old woman. In his appeal he claimed that the circuit court had wrongfully accepted telephone records of his calls as evidence, despite the fact that it could not be established if these were maintained during regular course of business or represented hearsay. The court stated that the telephone records were not the counterpart of a statement by a human witness, which would ideally be tested by cross-examination of that witness. Such evidence would not be treated as hearsay and its admissibility would be determined by the reliability and accuracy of the process involved. The appeal was dismissed because this case indeed confirmed that a proper process had been followed to obtain the digital evidence. The case is important as it established one more precedent of the enormous importance of a reliable and accurate process to be followed when producing digital evidence.

It is worthy to note that although there are a few cases where courts explicitly analysed whether a correct digital forensic investigation process had been followed, this is still not common practice. Most courts usually enquire about tools and methods used, but they rarely concentrate on the process. In the author’s opinion, this is creating a gap and the possibility exists that wrongful evidence can be accepted and presented as digital evidence. Furthermore, the author believes that as the digital forensic field advances and becomes more important and versatile (think of cloud forensics, mobile forensics, network forensics), the courts will eventually have to examine the digital forensic investigation process used on a regular basis. This is especially true in view of the recently published related ISO standard, ISO/IEC 27043:2015 [21].

If a standardised digital forensic investigation process were to exist, it could help bridging the gap between different jurisdictions in relation to the requirements for a digital forensic investigation process. Requirements for admissibility may vary considerably between jurisdictions and for this reason it is highly advisable to obtain competent legal advice regarding the particular jurisdiction’s specific requirements. Nonetheless, many jurisdictions

include at least the following two aspects in their admissibility requirements for evidence [21]:

- Relevance – the evidence must have some relevance to the facts in dispute.
- Authenticity – the evidence must be shown to be what it purports to be. For example, if a particular JPEG (Joint Photographic Expert Group) image extracted from the hard drive of a particular server is relevant to a question of fact under dispute, the trier of fact will demand demonstrable assurance that the drive belongs, in fact, to that particular server, that it has not been modified in any way since its collection, that the process used to extract the JPEG image is trustworthy, etc.

The following section concludes the chapter.

3.3 Conclusion

In this chapter the author provided information on legal aspects relating to a digital forensic investigation process. Without intending to promote the specific legal systems of particular countries, the author presented the following:

- The most important rules and guidelines (Daubert [20], ACPO [51])
- Examples of court cases [22,23]
- General requirements for admissibility of digital evidence [21]

The author's aim was to support the statement that there is a need and requirement to follow a formalised and (ideally) a standardised digital forensic investigation process while performing an investigation.

Based on this identified need, and taking into account existing state-of-the-art digital forensic investigation process models from different countries and legal jurisdictions, the author is proposing a model that not only harmonises existing models and introduces important novelties, but would also ultimately lead to standardisation in this field.

The next part of the thesis, **Part 3: Model**, will propose a comprehensive and harmonised digital forensic investigation process model.

PART 3: MODEL

Part 3 of this thesis comprises three chapters (**Chapters 4, 5 and 6**). The first chapter proposes a comprehensive and harmonised digital forensic investigation process model that ultimately aims to achieve standardisation in the field. The proposed model is inclusive of readiness processes. It also proposes the introduction of a novel process class called *concurrent processes*, which constitutes a major contribution to the field.

The second chapter of **Part 3** concentrates on a comparison of existing state-of-the-art models (presented in **Part 2** of the thesis) with the proposed model in order to show the comprehensiveness, holistic approach and benefits of the proposed model.

In the final chapter of **Part 3**, the author analyses the results of implementing the proposed process model by using real-world cases so as to evaluate the usability and effectiveness of the proposed process model.

CHAPTER 4- A COMPREHENSIVE AND HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS MODEL

4.1 Introduction

In this chapter the author presents and proposes a comprehensive and harmonised digital forensic investigation process (DFIP) model. It is important to note that the proposed process model includes processes aimed at achieving digital forensic readiness in order to portray a comprehensive approach to the digital forensic investigation process and achieve the best investigation effectiveness and efficiency. The author also introduces a novel class of processes called *concurrent processes*, which are defined as the investigation processes that run in conjunction with other processes within the harmonised process model. These novelties, together with the comprehensiveness of the proposed process model, are important contributions to the field as they represent significant improvements.

The aim of the proposed model and guidelines is to expedite investigations by making available proper guidelines for guiding an investigator through the order of events during an investigation. Such guidelines would also be a good starting point to encourage the training of inexperienced investigators. The former should promote guidance on the process to be followed during any kind of digital investigation in such a way that, if challenged in any court of law, no doubt should exist as to the correctness of the investigation process followed by the investigation.

The following section discusses the methodology used to construct the proposed model.

4.2 Methodology

In order to create a comprehensive and harmonised digital forensic investigation process model, the author based the methodology to be applied on a comprehensive literature survey. The author studied the available literature within both the academic and industrial domains to identify the models currently used for the digital forensic investigation process. To the best of the author's knowledge, all existing and relevant models were studied in detail, with the exception of those that have not made significant contributions and/or are not used widely in the industry and academic environment. Documents studied were from different countries

and different legal jurisdictions, with some being academic work and others being guidelines and procedures published by Government agencies.

Existing models were studied according to their attributes such as structure, tiers, scope, scope processes (phases), number of processes (phases), order of processes (phases) and uniqueness of processes (phases).

As indicated here, the term “phases” are often used in literature to refer to processes within the digital forensic investigation process. In this thesis, the author refers to the steps as “subprocesses”, or simply “processes”.

Based on an analysis of the results of this study, the author defined the comprehensive harmonised digital forensic investigation process model. The aim was to harmonise the existing models and achieve comprehensiveness by adopting a holistic approach towards the digital forensic investigation process in general.

Furthermore, through the author’s engagement with the International Standardization Organization, the proposed process represented the single main input to the creation of an international standard in this field [21]. Hence, the proposed holistic process, the individual processes and the principles applied, passed significant public scrutiny from esteemed information security experts, which expedited the author’s final proposition for the comprehensive and harmonised digital forensic investigation process model.

Also, the effectiveness and usability of the proposed model was verified through use cases and evaluation of the proposed implementation prototype, as will be explained in the chapters to follow.

The author’s proposal for a harmonised digital forensic investigation process model is presented in the following sections.

4.3 A comprehensive and harmonised digital forensic investigation process model

The digital investigation process model consists of several processes. Each of these processes is generic enough and described at such a level of abstraction in this thesis that they can be used for different types of digital forensic investigation and for different types of digital evidence. Also, the model is comprehensively harmonised, meaning that it is inclusive of the

benefits of all the previous models examined during this research. Processes have been selected based on previous work in this field, in both the industry and academic environment. An attempt was subsequently made to harmonise the processes described by other authors and organisations.

The new harmonised model inherits most of the processes proposed by other authors and introduces additional processes and process classes. In that sense, it is comprehensive. It also proposes a harmonised organisation of the processes, while introducing a novel approach in the way some of the processes are implemented, i.e. *concurrent processes*. The author defines concurrent processes as the principle actions that should be achieved in parallel with other processes within the digital forensic investigation process model. The author believes that the introduction of a class for concurrent processes is a significant contribution, because the introduction of such a class of processes would not only enable more efficient and reliable investigations to take place holistically, but also promote strict adherence to the digital forensic investigation principles.

The following principle was used to distinguish between different processes: A set of activities can be defined as a process if all activities have a common aim and if the activities last for a limited period of time [26].

In order to abstract all processes on a higher level, all digital forensic investigation processes in the harmonised model are categorised into the following digital forensic investigation process classes [21]:

- Readiness processes class
- Initialisation processes class
- Acquisitive processes class
- Investigative processes class
- Concurrent processes class

These classes are discussed in the following sections, starting with an overview of the proposed classes so as to allow the reader to first gain a holistic view of the model and its

classes. In addition, one should also then be able to understand the basics about each of the classes as well as how these classes are related before drilling down into the details.

4.4 Overview of the digital forensic investigation process classes

In order to abstract the digital investigation processes at a higher level, these processes can be categorised in terms of digital investigation process classes. An overview of their relations is shown in **Figure 4.1**.

The *readiness* class of processes deals with pre-incident investigation processes aimed at achieving digital forensic investigation readiness within an organisation. The processes in this class attempt to maximise the use of potential digital evidence, whilst minimising the costs and interference with business processes. This class of processes should also enable preserving or improving the information security of potential digital evidence. Note that the readiness processes are optional to the rest of the digital forensic investigation processes. The reasons for this are explained in more detail in **Section 4.5**. However, the main reason why the readiness processes are optional is because the readiness processes are proactive compared to the rest of the investigation processes (which are re-active in nature).

The next three classes include the *initialisation processes*, *acquisitive processes* and *investigative processes* respectively. All these classes follow one another and do not overlap in time. As shown in **Figure 4.1**, however, the *concurrent processes* class runs in parallel with all other classes, ensuring the application of digital forensics principles.

The *initialisation* class of processes deals with the initial launch of the digital forensic investigation. The processes in this class are concerned with incident detection, first response, planning and preparation of the actual digital forensic investigation. They are of extreme importance for the success and effectiveness of the investigation, as they represent the basics and foundation for any of the processes that follow the initialisation processes. If any error or omission is made during these processes, digital evidence may become unusable or unavailable, and the integrity of the entire process may be endangered. For example, if during first response, the first responder shuts down a computer that contains digital evidence, digital evidence from RAM memory might be lost, or if one does not prepare for potential digital evidence collection and acquisition, the investigation may encounter difficulties at later stages (loss of time, resources, or even potential digital evidence).

The *acquisitive* class of processes deals with the physical scene investigation. Processes in this class are concerned with the acquisition of digital evidence. The validity and relevance of digital evidence depend heavily on these processes, and during these processes the integrity of digital evidence may be compromised or important evidence may be overlooked.

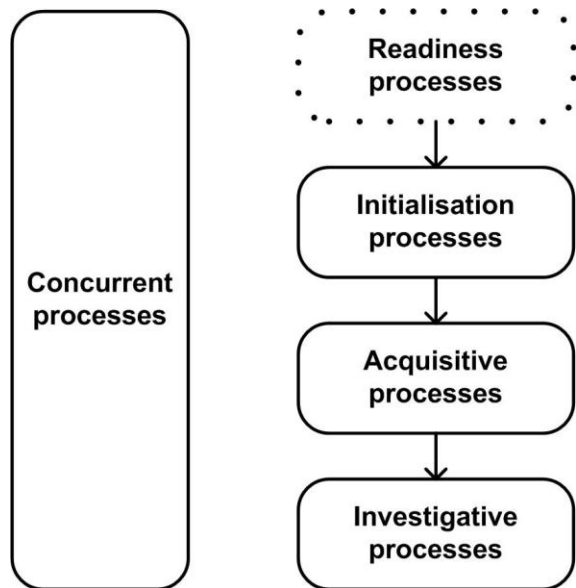


Figure 4.1 Classes of the proposed model

The *investigative* class of processes deals with uncovering the potential digital evidence and it includes processes aimed at examination and analysis, interpretation, reporting, presentation and investigation closure.

The *concurrent* class of processes takes place concurrently with all the other processes mentioned above. Concurrent processes are defined as the principles that should be applied throughout the digital forensic investigation process, since such concurrent processes are applicable to many other processes within the digital forensic investigation process. These processes are important as they ensure that digital forensic principles are implemented and abided by, hence ensuring proper digital evidence admissibility and greater investigation effectiveness. The concurrent processes are aimed at achieving the highest possible efficiency of the investigation and to ensure the admissibility of digital evidence. Translating these principles into actionable items makes it easier for practitioners to adhere to them strictly.

The sections that follow provide a detailed explanation of each of the digital forensic investigation process classes mentioned above.

4.5 Readiness processes

This class of processes, as mentioned before, is optional to the digital forensic investigation processes and it is affected by organisations rather than investigators. An organisation might decide whether to implement a digital forensic readiness process or not, depending on its internal policies, available resources, legal environment and specific circumstances. The rest of the process classes can be implemented even if the *readiness processes* class has not been implemented. It should be mentioned that future legislation (in applicable jurisdictions) and/or corporate governance guidelines might compel organisations to implement the readiness processes as well, at least to some level, due to the rise in the number of cyber-attacks across the world. In his effort to harmonise the digital forensic investigation processes, the author adopted and defined the following aims for a readiness processes class, which were harmonised mostly from previous work [24, 42, 43, 44, 48, 63-65]. The only exception was the last aim, which was added by the author and represents a novel approach and a contribution of the thesis. The processes in this class should achieve the following:

1. Maximise the potential use of digital evidence
2. Minimise the costs of digital forensic investigations incurred
3. Minimise interference with and prevent interruption of business processes
4. Preserve or improve the current level of information security

The author firmly believes that aim 4 should also be taken into account when implementing readiness measures. This is a novel requirement introduced by the author to achieve a more holistic approach from the point of information systems security.

It is not viable to concentrate only on efficiency of the investigation (aims 1 and 2) and non-interference with business processes (aim 3), because achieving only the first three aims could still leave room for flaws in the overall information security status of an organisation. An example of such a flaw is when (based on the first three aims) an organisation decides to collect logs from its information systems, keeps them at a central location and does not envisage security mechanisms for sufficiently protecting such data – which might lead to the compromise or leakage of the data. It is, therefore, necessary to adopt a more holistic approach by applying the CIA (Confidentiality, Integrity, Availability) information security

principles. The author believes that the harmonised model should have built-in security features and that security should not merely be an add-on.

Figure 4.2 depicts the *readiness processes* class as described above, refined into process groups as follows: The class of *readiness processes* consists of three distinctive readiness process groups, namely the *planning processes group*, the *implementation processes group* and the *assessment processes group*.

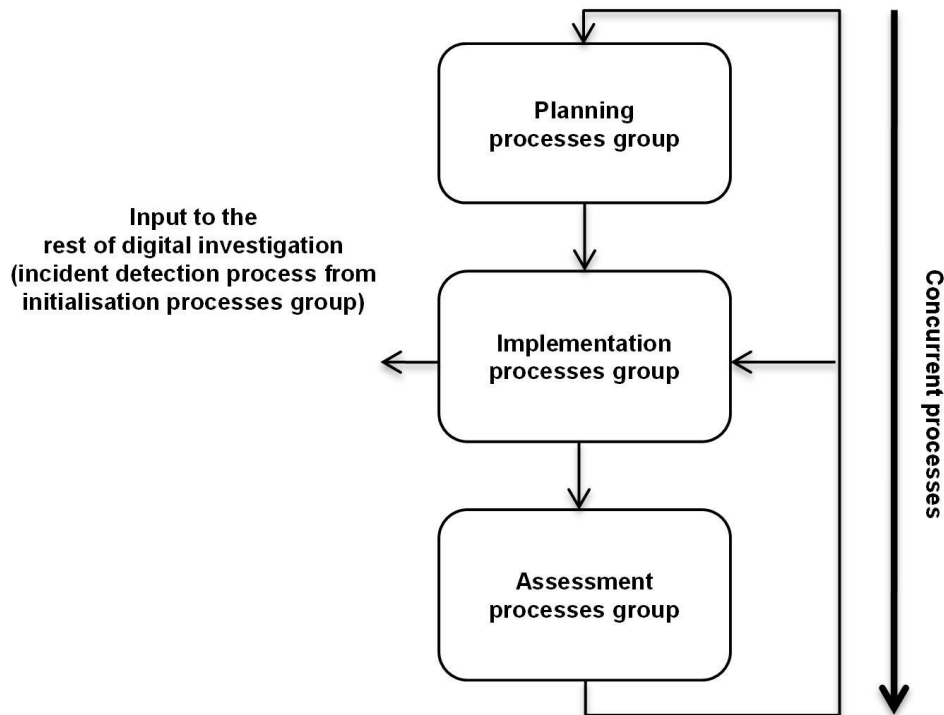


Figure 4.2 Readiness processes groups

The *planning processes* group includes all readiness processes that are concerned with planning activities, including *scenario definition*; *identification of potential digital evidence sources*; *planning pre-incident collection*; *storage and handling of data representing potential digital evidence*; *planning pre-incident analysis of data representing potential digital evidence*; *planning incident detection*; and *defining system architecture* – all depicted in **Figure 4.3**.

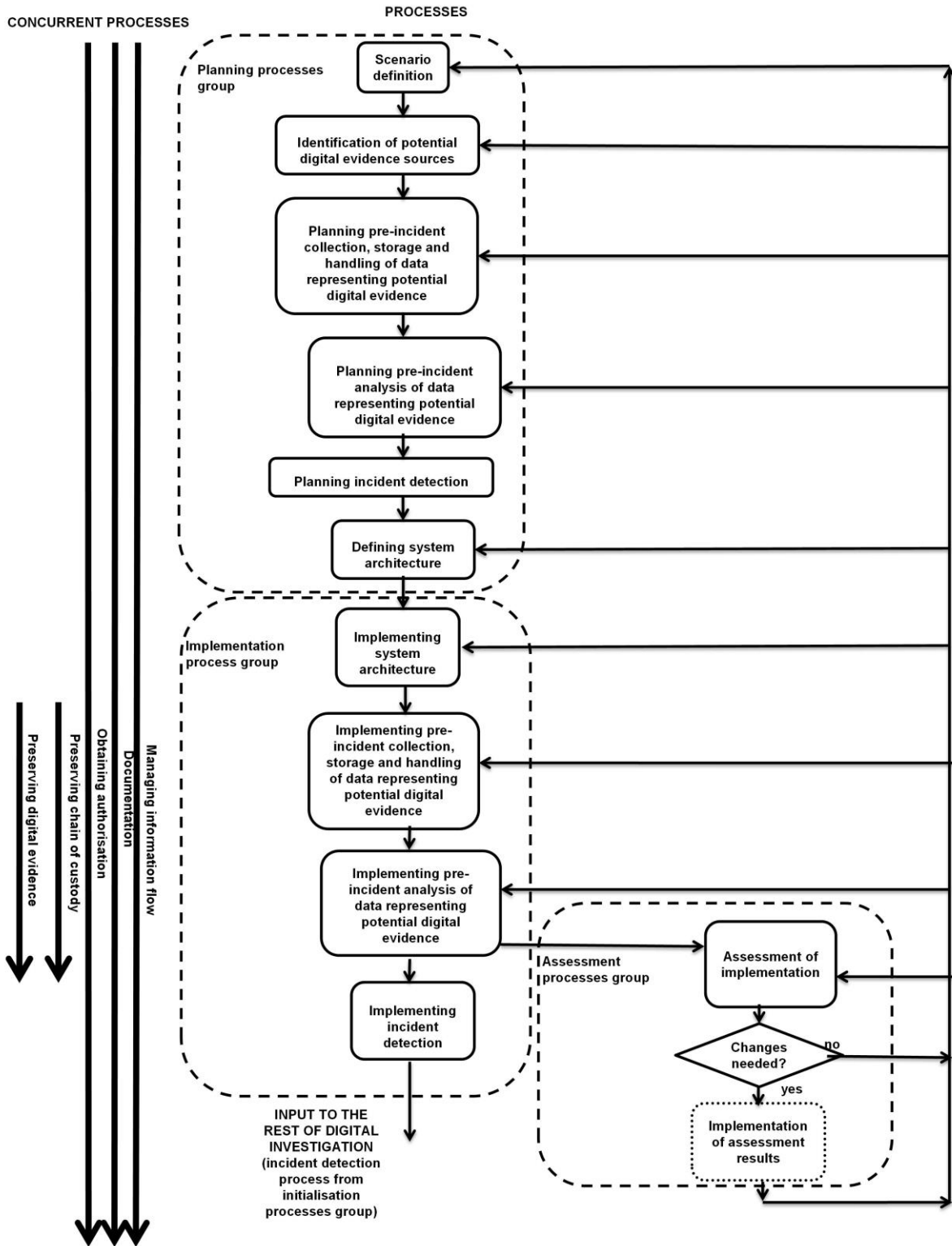


Figure 4.3 Readiness processes

The *implementation processes* group includes the following readiness processes: *implementing system architecture; implementing pre-incident collection, storage and*

handling of data representing potential digital evidence; implementing pre-incident analysis of data representing potential digital evidence and implementing incident detection, as shown in **Figure 4.3**. These processes are concerned with the implementation of the results of the planning processes.

The *assessment processes* group includes two readiness processes, namely *the assessment of implementation* and *the implementation of assessment results*. The *implementing incident detection* process links to the *incident detection* digital forensic investigation process as shown in **Figure 4.7**.

Note that the processes are defined at a high level in order to be used as a model for different types of Digital Forensic Investigation (DFI). The author does not attempt to prescribe what exactly each of the processes should entail. There exist many different types of DFI, such as live forensics, cloud forensics, network forensics and mobile forensics. The author believes that detailed procedures for each subsequent process should be defined for each specific type of DFI; however, doing so does not fall within the scope of this thesis. The harmonised model should therefore be used as an “umbrella” model for each of the different DFI types, i.e. the detailed procedures are to be implemented by other standards and DFI practitioners.

Input to all processes in **Figure 4.3** includes all information regarding system architecture, technology (hardware and software), policies, procedures and business processes of an organisation, where applicable. The input must also consider the four aims for the readiness processes as mentioned earlier. The input arising from the mentioned four aims is referred to as pre-known system inputs in the remainder of the thesis. For example, pre-known system inputs may include network topology of the system; specification of models and components of hardware used; specification of firmware; operating systems and applications for each piece of hardware (if applicable for the hardware in question); information security policies that are in place regarding the use of the system; and description of business use of the system in question.

The readiness processes are iterative, which implies that after the last process one can return to previous readiness processes, as shown in **Figure 4.3**. For example, when during the *assessment of implementation* process one notes that certain defined system architecture was not properly implemented, one would need to go back to the *implementing system architecture* process. Also, if one notes that plans made during the *planning pre-incident*

collection, storage and handling of data representing potential digital evidence process are not in line with aims for having digital forensic investigation readiness processes in the particular organisation, one could go back to the *planning pre-incident collection, storage and handling of data representing potential digital evidence* process to change those plans accordingly.

Each of the readiness processes are explained in the subsections that follow.

4.5.1 Scenario definition

As part of this process one should examine all scenarios where digital evidence might be required. The output of this process includes the defined scenarios, which might be scenarios of information security incidents such as the unauthorised use of resources, or scenarios of other events that, as a consequence, require a digital forensic investigation, such as investigating the use of a computer to distribute child pornography.

It is also recommended that during this process a proper risk assessment be performed for each identified scenario. A risk assessment would allow the better identification of all possible threats, vulnerabilities and related scenarios that would expose particular information assets. Based on the assessed risk from certain threats, vulnerabilities or scenarios, one can, in later processes, better decide on the required controls to achieve investigation readiness within an organisation. This would enable an organisation to take into account the risk level, costs, and benefits of possible controls in a bid to reduce the identified risk.

The *scenario definition process* is a logical start for the *readiness processes class*, as it provides for the laying of the foundation needed for all further process through proper scenario analysis. After this initial process, one should define all possible sources of digital evidence, based on the scenarios defined within this process. The *sources identification process* is again a prerequisite for further processes that deal with the handling of potential digital evidence.

4.5.2 Identification of potential digital evidence sources

In this process one should identify all potential sources of digital evidence within an organisation. The output of this process is the defined potential sources of digital evidence. Some of the identified potential sources might not be available. For example, unless access logs are introduced into the system, they would not be available as a source of data in the case of a digital forensic investigation. In that case, controls should be explored to make the identified source available.

After the potential digital evidence sources have been identified, one should define or determine how these sources would be handled. Therefore, the next two processes, which are explained in the next two subsections, include *planning pre-incident collection, storage and handling of data representing potential digital evidence* and *planning pre-incident analysis of data representing potential digital evidence*.

4.5.3 Planning pre-incident collection, storage and handling of data representing potential digital evidence

In this process one should define activities for pre-incident collection, storage and handling of all data that represents potential digital evidence. The output of this process includes the defined activities for the pre-incident collection, storage and handling of such data.

The data collection period is to be determined by a risk assessment. For example, this could mean determining how often an organisation should save the application log to a central repository to ensure integrity of the log data in case the application is compromised. Also, note that the collection, storage and handling of data have to conform to digital forensic investigation principles in order for digital evidence to be admissible in a court of law. Lastly, the retention period of data is to be determined based on the following factors:

1. Risk assessment
2. Previous experience regarding incident detection, data quantities, network capacity and all other matters that could influence cost or efficiency of this process
3. Laws within the particular jurisdiction
4. Regulations
5. Business-specific requirements

4.5.4 Planning pre-incident analysis of data representing potential digital evidence

In this process one should define the procedures for pre-incident analysis of all data that represents potential digital evidence.

The input to this process includes the scenarios as defined in the scenario definition process, as well as the output from the pre-incident collection process. The input must also include the aims for the readiness processes.

The output of this process includes the defined activities for pre-incident analysis of the data that represents potential digital evidence. The aim of this analysis is to detect an incident. Therefore, activities defined in this process must include exact information on how the incident is detected and what behaviour constitutes an incident. As the output of this process is delivered in the form of detected incidents, this links to the input of the incident detection process of the digital forensic investigation processes as shown in **Figure 4.3**.

As the task of data analysis and incident detection often falls outside the scope of the functionalities of targeted information systems, it is recommended that this process defines an interface between the readiness processes and a monitoring system, which would analyse data in order to detect incidents. The monitoring system can be any system that is dedicated to this purpose. It can also be any one of the following systems: intrusion prevention systems; intrusion detection systems; change-tracking systems; log-processing systems, etc.

4.5.5 Planning incident detection

In this process one should define actions to be performed when an incident is detected. The output of this process includes defined actions to be performed once an incident has been detected, in particular information to be passed on to the rest of the digital forensic investigation process. Information should also include pre-known system inputs, results from all of the readiness class processes, as well as data gathered and generated during the *implementation process group* processes.

4.5.6 Defining system architecture

In this process one should define information system architecture for the organisation, while taking into account the output results of all previous readiness processes. The author

introduces this process to facilitate better results of the DFIR implementation and takes into account all relevant matters when redefining the system architecture.

Input to this process comprises the results from all previous readiness processes. The input must also include the aims of the readiness processes.

The output of this process is the defined system architecture for the organisation. The aim of this process is to customise system architecture to allow for the accomplishment of the aims of the readiness processes.

After the system architecture has been defined, one should embark on the implementation of conclusions and results that have emerged from all the processes performed.

Next, one should proceed with processes from the *implementation processes group*.

4.5.7 Implementing system architecture

In this process one should implement the system architecture as defined in the *defining system architecture* process. The output of this process is the implemented system architecture. Examples of *implementing system architecture* include the installation of new software, hardware and/or policies that would permit the remainder of the readiness processes to be instantiated across the information system and the organisation.

4.5.8 Implementing pre-incident collection, storage and handling of data representing potential digital evidence

In this process one should implement the pre-incident collection, storage and handling of data that represents potential digital evidence, as was defined in the *planning pre-incident collection, storage and handling of data representing potential digital evidence* process. The output of this process involves *implementing the pre-incident collection, storage and handling of data representing potential digital evidence*.

Examples of *pre-incident collection, storage and handling of data representing potential digital evidence* include the implementation of logging software and hardware, with time-stamping and digital signature mechanisms in place, or the implementation of customised software to collect the data of importance (i.e. system usage data).

4.5.9 Implementing pre-incident analysis of data representing potential digital evidence

In this process one should perform a pre-incident analysis of data that represents potential digital evidence, as defined in the *planning pre-incident analysis of data representing potential digital evidence* process. The output of this process involves implementing the pre-incident analysis of data that represents potential digital evidence.

Examples of *pre-incident analysis of data representing potential digital evidence* include the implementation of change-tracking software, intrusion detection/prevention software and/or anti-virus software.

4.5.10 Implementing incident detection

In this process one should implement the actions defined in the *planning incident detection* process. The implementation of incident detection also depends on and receives input from the process entitled *implementing pre-incident analysis of data representing potential digital evidence*, as detection occurs based on the analysis performed.

During the *implementing incident detection* process, detection of an incident occurs according to the rules defined in the *planning incident detection* process. Moreover, during the *implementing incident detection* process, one should decide which data pertaining to the incident should be passed on to the rest of the digital forensic investigation process.

Examples of incident detection are when change-tracking software detects changes in a certain archived log or when an intrusion is detected via an intrusion detection system.

Requirements for an event to be declared an incident that requires digital forensic investigation would depend on the policies of the organisation and cannot be prescribed by this thesis.

Implementing incident detection process represents an interface with the rest of the digital forensic investigation process, as it constitutes an overlap between readiness processes and an investigation itself. The reason for overlap is that a digital forensic investigation cannot start until an incident has been detected.

4.5.11 Assessment of implementation

In the *assessment of implementation* process, one performs an assessment of the results of the *implementation process group* and compares these to the aims for achieving digital forensic investigation readiness.

The output of this process is the results of the assessment of implementing digital forensic investigation readiness for an information system. It is recommended that during this process a legal review should be carried out for all procedures, controls and architectures defined previously. The review should show, among others, whether there is conformity with the legal environment and digital forensics principals of the particular jurisdiction, in order to ensure admissibility of the potential evidence in court.

4.5.12 Implementation of assessment results

This process is concerned with the implementation of the conclusions obtained from previous processes. Note that this process is optional, as it is possible that no changes are needed, based on the *assessment of implementation* process.

In **Figure 4.3**, this process is marked as optional and indicated as such with a dashed line around the process.

During this process one should decide on recommendations for changes in one or more of the previous processes. The main decision here is whether to go back to one of the planning processes in the *planning processes group* of the *readiness class* of processes, or to go back to one of the processes in the *implementation process group*, depending on the conclusions of the *assessment of implementation* process. For example, one might conclude that the implementation of a certain measure (i.e. that during *implementing system architecture*, one has not properly implemented log-in authorisation controls planned during the *defining system architecture* process) was not performed in an optimal manner, or one might decide that a new implementation has to be performed.

4.6 Initialisation processes

This next class of processes deals with the initial commencement of the digital forensic investigation including *incident detection*, *first response*, *planning* and *preparation processes*.

4.6.1 Incident detection process

Incident detection procedures must be in place prior to the beginning of this process. The procedures can define the relation between the information system where the incident might occur and the external information system that would have the task to detect an incident or define how humans operating or administering information systems detect an incident. Examples of external incident detection systems are intrusion detection systems, intrusion prevention systems, log-analysing systems, change-tracking systems, etc.

The *incident detection* process includes not only the detection of the incident, but also its classification and description, which has a significant influence on the rest of the process. For example, the digital forensic investigation would take a completely different course if the incident was described as ‘unauthorised access to the root account of the operating system’, than if it was described as ‘using the computer to distribute abusive images’. Based on the above, this process may consist of three sub-processes: incident detection, incident classification and incident description. It is important to note that the incident classification and incident description subprocesses should be performed based on information gathered prior to incident detection. However, it should not include any activity (i.e. running some data analysis software on the system) that might alter data at the information system in which the incident occurred, in order to preserve the integrity of the digital evidence.

Incident detection activities were defined since DFRWS [39] (as part of Identification process), but Mandia et al. [43] were the first to define these in a separate process. The author strongly believes that incident detection activities should be included as a starting point in the digital forensic investigation process. The reasoning behind selecting the incident detection process as a first process in the model (and not a preparation or planning process as some authors have suggested) is that the author believes that digital forensic readiness activities should exist in a process separate from a digital forensic investigation process, as digital forensic practitioners could never ensure that digital forensic readiness activities can be implemented on every system they would work on. (If preparation and planning for a digital forensic investigation would exist as activities prior to incident detection, they would form part of digital forensic readiness.) Therefore, the actual digital forensic investigation process starts with *incident detection* and *first response*, followed by *preparation* and *planning* processes.

4.6.2 First response process

The *first response* process should include the first response to the detected incident. Depending on the type and severity of the incident, this might include disconnecting equipment from a networked environment, detecting corrupted data, etc. This process should also include measures to ensure that volatile data is not lost. The first response should be performed in such a way to ensure it does not have a negative influence on the possibility to perform a successful digital forensic investigation, e.g. it should avoid powering off the equipment, opening or changing files on a live system, etc. Defining the *first response* subprocesses falls outside the scope of this document, as these can vary greatly depending on the type of target information systems, data contained in the target information system, circumstances of the incident, classification and description of the incident, etc. Mandia et al. [43] and Beebe and Clark [44] included incident response process in their models as initial response and incident response respectively. The author chose to include this process because he firmly believes that it must be part of the digital forensic investigation process to ensure the integrity of the digital evidence (for example to ensure that the first responder does not destroy or alter some of the digital evidence, i.e. application configuration files).

4.6.3 Planning process

During this process, the investigator has to perform all the planning needed for later in the digital forensic investigation process. Planning should include the development of relevant procedures, the definition of methodologies and tools to be used, planning for the use of appropriate human resources and the planning of all activities during other processes. If digital forensic investigation readiness controls were implemented, the investigator should plan how to use the results of those controls so as to maximise the success of the digital forensic investigation process. The *planning* process is included because it is of extreme importance due to the fact that it determines the efficiency and success of all the other processes.

4.6.4 Preparation process

Preparation process activities are intended to prepare an organisation for performing the activities of other digital forensic investigation processes. This might include – but are not limited to – the preparation of relevant equipment (hardware and software), infrastructure, human resources, raising awareness, training and documentation. During this process, preparations also have to be made to implement procedures defined in the previous process. The preparation process is included because such a process would ensure that the investigator is better prepared to carry out the acquisitive processes in an efficient manner. It would also ensure that the integrity of potential digital evidence is not compromised due to the possible ill preparedness of the investigator.

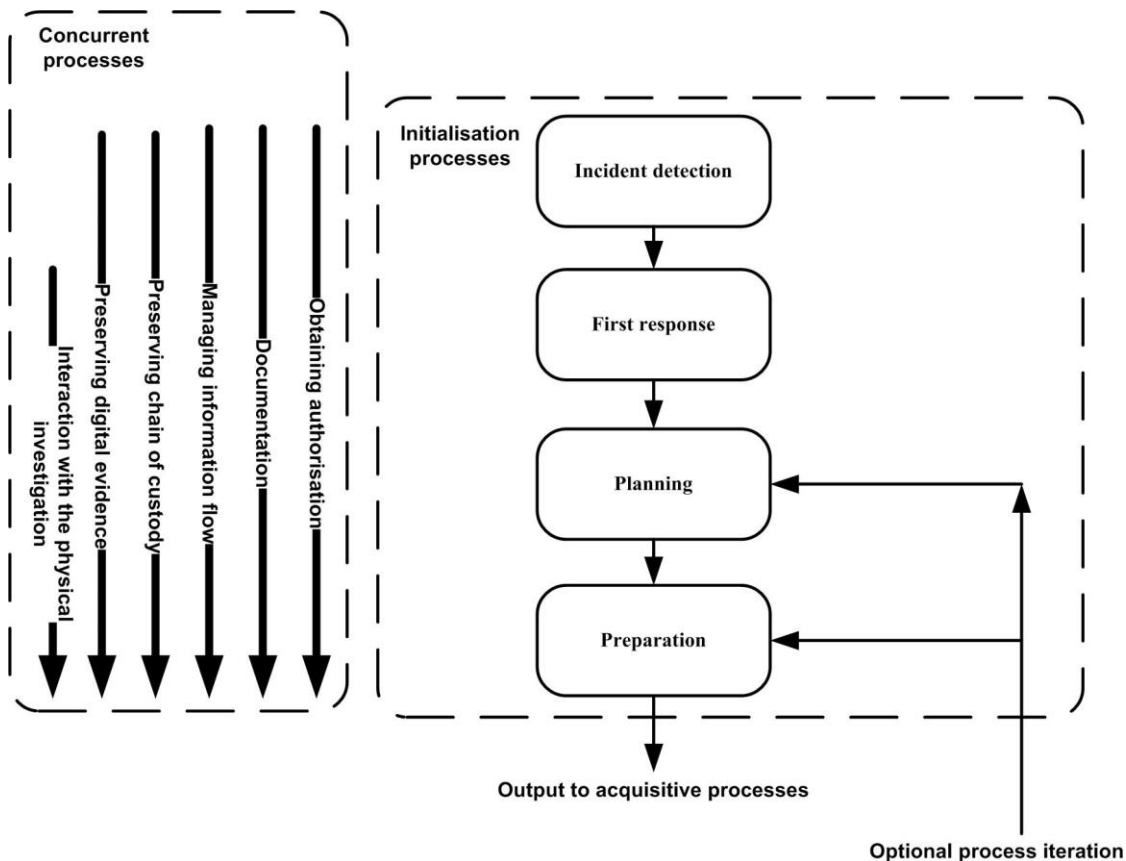


Figure 4.4 Initialisation processes

4.7 Acquisitive processes

The *acquisitive processes* class consists of processes that are concerned with the acquisition of digital evidence, as shown in **Figure 4.5**.

4.7.1 Potential digital evidence identification process

This is the first process performed at the scene of the incident. Although it overlaps in time with the previous process, it should be considered a separate process because it includes different types of procedures that have the specific aim of identifying potential digital evidence. Cohen says in [47]: “In order to be processed and applied, evidence must first, somehow, be identified as evidence. It is common for there to be an enormous amount of potential evidence available for a legal matter, and for the vast majority of the potential evidence to never be identified.” Identifying potential digital evidence at the incident scene is of crucial importance for the remainder of the process, because if potential digital evidence is not identified at this point, it might not even exist at a later point during the process. This is especially important when an incident happens in a networked environment, in an environment where live investigations should be performed, in a cloud environment, or in an environment with exceptionally large amounts of data to deal with. Researchers such as [40-42, 45-47, 51] included this process in their respective models, some under a different name or with a different scope. The author believes that the *potential digital evidence identification process* should be a separate process, with the sole aim to identify potential evidence.

4.7.2 Potential digital evidence collection process

Once potential digital evidence has been identified, it has to be collected to permit its analysis in a later process. Evidence must be collected in such a manner that its integrity is preserved. This is important if one needs to use this evidence at a later stage to draw formal conclusions, i.e. in a court of law. Adhering to strict legal regulations during the evidence collection process is of crucial importance, as digital evidence might become unusable when proper procedures are not followed. It is notable that many authors [39, 40, 47] have proposed two separate processes instead of *collection process* proposed by the author. In fact, they propose separate collection and preservation processes. However, the author believes that this should be a single process as it has only one aim, namely to reliably collect potential evidence. Please note that the preservation process proposed by [29,40,47] is a sequential process and it is different from the *preserving digital evidence* process proposed by the author, which is concurrent and runs throughout the duration of the investigation.

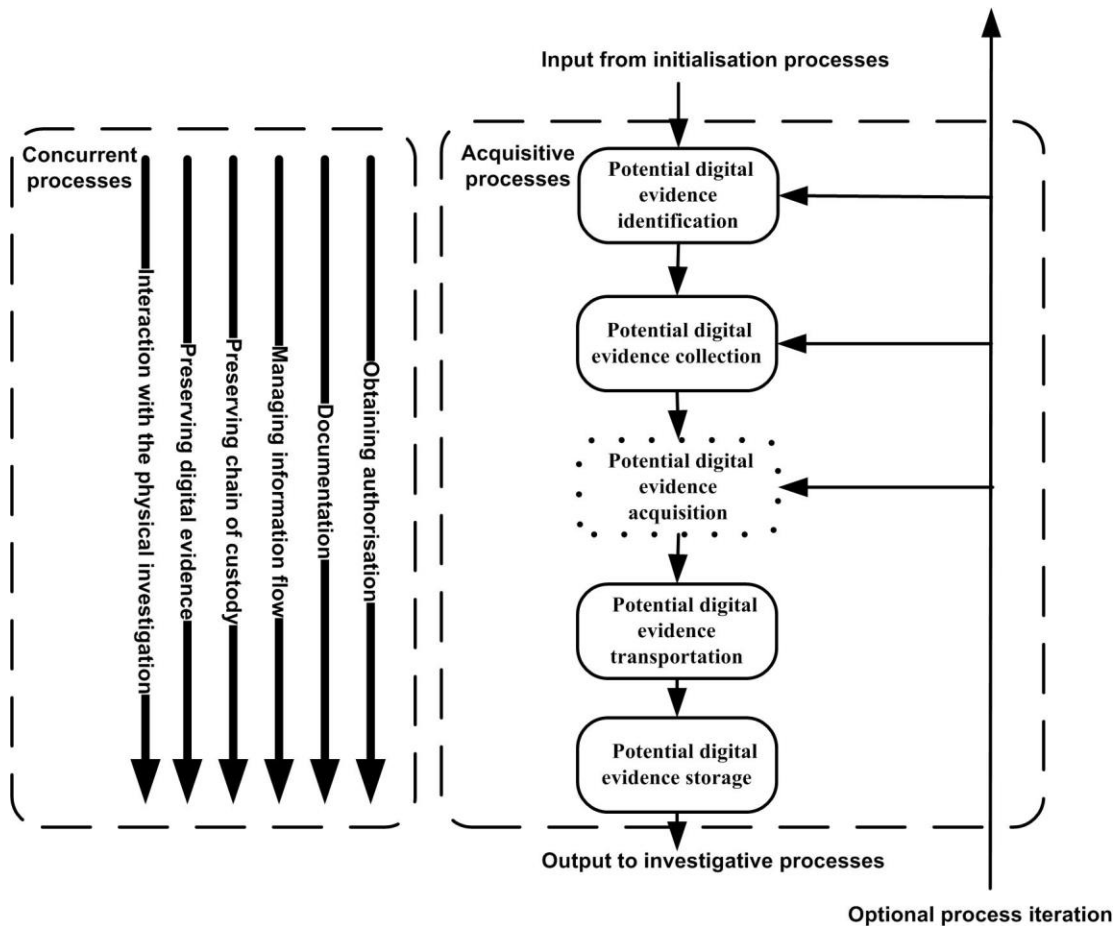


Figure 4.5 Acquisitive processes

4.7.3 Potential digital evidence acquisition process

Once potential digital evidence has been collected, it has to be acquired to permit its analysis in a later process [21]. Again, adhering to strict legal regulations during the potential digital evidence acquisition process is of crucial importance, as such evidence may become unusable if proper procedures are not followed. Take note that this process is optional at this stage, since it is not always possible to acquire one or more images of the evidence after it has been collected. It often happens that image acquisition only takes place within an investigation laboratory and, hence, this process might only take place within the *investigative processes* class [21].

4.7.4 Potential digital evidence transportation process

During this process, potential digital evidence is transported to a location where it is to be stored and later analysed. Transportation can be done physically or electronically. If the evidence is transported electronically, special precautions have to be taken to preserve the integrity, confidentiality and chain of custody, such as encrypting and digitally signing data. In various sources [41, 45, 47] this is included as a separate process. Transportation should exist as a separate process on the basis that activities performed have a single aim (not shared with other processes), namely to securely transport the potential evidence to the location where analysis will be performed, while complying with the principle of preserving the integrity of the evidence.

4.7.5 Potential digital evidence storage process

The storage of potential digital evidence may be needed if analysis cannot be performed right away or if there is a legal requirement to keep the digital evidence for a certain period of time. Preservation of the integrity of the evidence and the chain of custody is of utmost importance during this process. Care must also be taken not to damage the media containing potential digital evidence through factors such as shock, temperature, humidity, pollution, loss of power, malfunction, etc. In various sources [45, 47, 51] storage is included as a separate process. It should exist as a separate process on the basis that activities performed have a single aim (not shared with other processes) to securely and safely store the potential evidence.

4.8 *Investigative processes*

The *investigative processes* class consists of processes that are concerned with investigating the incident that is the cause of the digital forensic investigation. It is focused on analysing the evidence, interpreting the results of the analysis, writing a report on the results of the *digital evidence interpretation* process, and presenting these results in a court of law or to the relevant parties involved. Finally, the digital forensic investigation draws to a close within the *investigation closure* process.

4.8.1 Potential digital evidence acquisition process

If this process was not performed during the execution of the acquisitive processes class, it is performed at this stage. See *potential digital evidence acquisition* process again for details in **Section 4.7.3**.

4.8.2 Digital evidence examination and analysis process

Analysis of the potential digital evidence involves the use of a large number of techniques to identify digital evidence and reconstruct the evidence, if needed. The aim is to formulate a hypothesis on how the incident occurred, what its exact characteristics are and who is to be held responsible. Formulating a hypothesis basically involves the reconstruction of the sequence of events that led to the current state of the system being investigated. Due to the volume, diversity and complexity of the data to be analysed in present-day digital forensic investigations, the analysis of evidence becomes a challenge. As volumes of data to be analysed can be vast, automated techniques are often employed to complement manual analysis techniques. Some of the researchers in this field have split the scope of the proposed *digital evidence examination and analysis* process into several separate processes [39, 41, 51]. The author nonetheless decided to propose a single process whose aim would be to produce a hypothesis about incident occurrence and find appropriate digital evidence to support the hypothesis.

4.8.3 Digital evidence interpretation process

The results of the *digital evidence examination and analysis* process should next be interpreted during this process. Interpretation of any evidence is dependent on the information available about the circumstances surrounding the creation of that item of digital evidence. To be able to make a proper interpretation, information from persons involved in the day-to-day running of the system(s) being investigated is often required. Furthermore, information about the purpose of the investigation and a definition of the scope of the investigation are also required. One goal of the *digital evidence interpretation* process is to use scientifically proven methods to explain the facts revealed during the *digital evidence examination and analysis* process, within the context of the investigation, thus enabling one to confirm or dispute the hypotheses set in the previous process. If the contextual information changes, the interpretation may also have to change in order to reflect such contextual information changes. A further goal of the digital evidence interpretation process

is to classify the interpreted evidence according to its relevance. This means that the evidence, as interpreted, is organised in such a way that one may distinguish which digital evidence artefacts are more important than others. The process of deciding which pieces of digital evidence would be more important than others is left to the discretion of one or more competent investigators [21].

4.8.4 Reporting process

Reporting represents the interpretation of the results of the previous process and should be the main result of the investigation. Due diligence should be exercised to list all relevant digital evidence in the report to assure that no valuable evidence is omitted [21]. The report may be distributed to different stakeholders, such as judicial system representatives, system owners, system custodians, etc. It is recommended in [21] that the report should elaborate on issues such as the potential evidence that was collected or acquired, the analysis techniques that were performed, the conclusions and findings that were taken into account, and the outcome that resulted from the report.

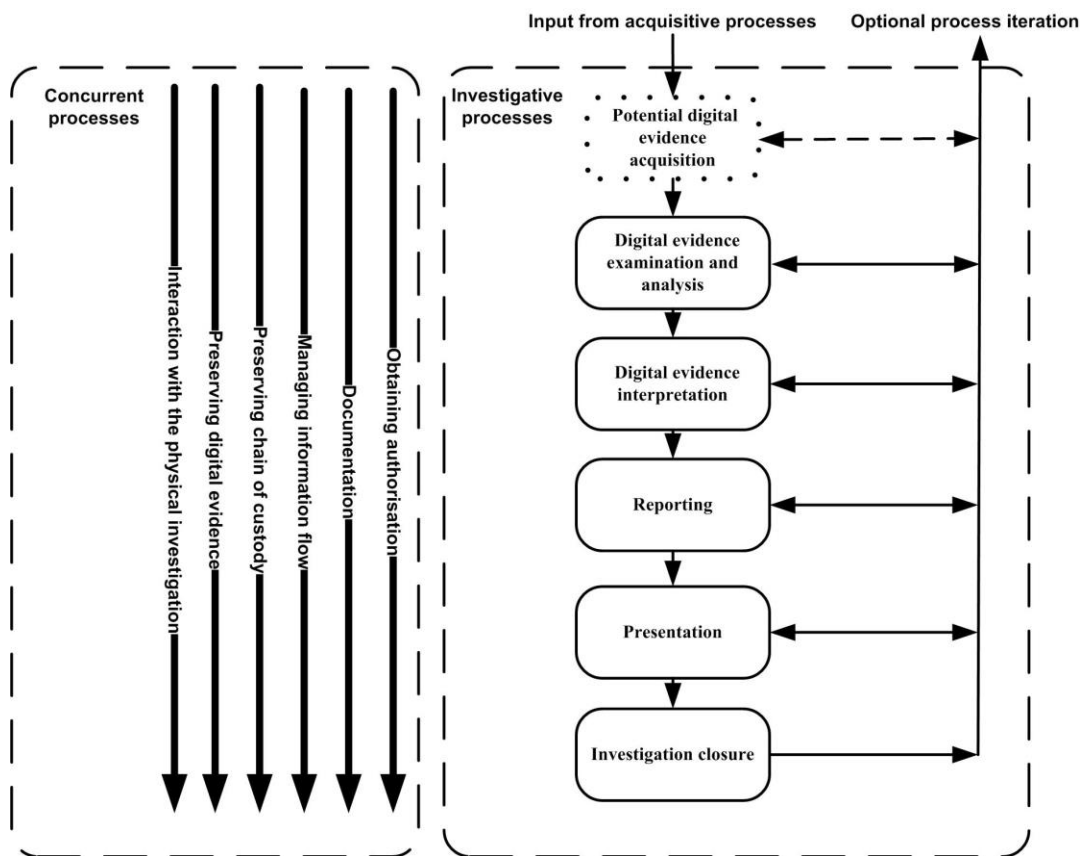


Figure 4.6 Investigative processes

4.8.5 Presentation process

The document created during the *reporting* process is to be presented to all stakeholders. In the case of a court case, the stakeholders include the judge, jury, accused, lawyers and prosecutors, as well as any other interested party. In the case of an internal company incident, stakeholders may be the company management team, shareholders and employees involved. The hypothesis that results from the analysis phase is to be presented together with the identified digital evidence. (Note that not all the identified potential digital evidence should be presented – only the evidence that is relevant and of importance for the hypothesis.) The presentation process also includes proving the validity of the hypothesis if or when the hypothesis is challenged. Thus, the one who presents the hypothesis should be prepared for such challenge. Most of the researchers whose work was studied in the literature survey included reporting as a separate single phase and the author believes that this is the correct interpretation of associated activities.

4.8.6 Investigation closure process

This process concludes the investigation and a decision is to be made on the validity of the hypothesis set in the presentation process. The digital forensic investigation process is iterative. This implies that – after completing this process – one can go back to any of the earlier processes that follow the *first response* process. The closing process should include the following subprocesses: Deciding on need to iterate to a previous process; Acceptance or rejection of the hypothesis; Returning evidence, if needed; Destruction of evidence, if needed. It should be noted that different laws apply in different jurisdictions. The way in which evidence is destroyed, whether it is destroyed, or whether it needs to be stored for a certain period of time after the case has been completed, all depends on the applicable local laws, rules and guidelines. The investigator should take cognisance of this fact. The distribution of relevant information to all stakeholders (i.e. communicating the need to iterate to a previous process, deciding on the acceptance or rejection of the hypothesis, or providing any reports or documents from the *presentation* process) should also be performed as part of this process.

4.9 Concurrent processes

In addition to the digital forensic investigation processes, the following processes are included to be considered concurrently with the digital forensic investigation processes:

obtaining authorisation [42, 45, 51]; *documentation* [40-47, 51]; *defining the information flow* [45, 51]; *preserving chain of custody* [20, 41-47, 51]; *preserving digital evidence* [20, 40-47, 51]; *interaction with the physical investigation* [42, 51]. Concurrent processes are defined as the principles that should be applied throughout the digital forensic investigation process, since such processes are applicable to many other processes within the digital forensic investigation process. For example, *documentation* is a concurrent process that is applicable to all processes within the digital forensic investigation process, since all tasks carried out during the entire digital forensic investigation process should be thoroughly logged and documented. The concurrent processes suggested above are justified, since the principles of the digital forensic investigation process, as well as the preservation of the evidence and the chain of custody should be translated into actionable items. These processes should run concurrently with all other processes to ensure full admissibility of the digital evidence in a court of law. Moreover, legacy processes (such as *obtaining authorisation*, *documentation* and *interaction with the physical investigation*) should actually run across several or all processes. The aim of these concurrent processes is to achieve higher efficiency of the investigation. *Information flow* should also be defined as a separate concurrent process.

The concurrent processes are explained in more detail next.

4.9.1 Obtaining authorisation

Proper authorisation should be obtained for each process performed as part of all of the digital forensic investigation processes. Authorisation might be required from government authorities, system owners, system custodians, principals, users, etc. It is important to obtain proper authorisation for actions performed during the digital forensic investigation process in order not to infringe on the rights of system owners, custodians, principals or users, but also to ensure that no legal rule is infringed. The required authorisations would depend on the environment where the digital forensic investigation is performed, both within a legal and an organisational environment.

4.9.2 Documentation

Each process performed should be documented to preserve the chain of custody, but also to improve efficiency and ensure the higher probability of a successful digital forensic investigation. Proper documentation must furthermore be demonstrated during the presentation process.

4.9.3 Managing information flow

A defined information flow should exist between each of the processes and among different stakeholders. This information flow has to be defined for each type of investigation. It is important to identify and describe information flows so that they can be secured and supported technologically. For instance, an information flow could refer to the exchange of digital evidence between two investigators involved in the same investigation. Protection of this information flow can for instance involve the use of trusted Public Key Infrastructure (PKI) [70,71] to identify the different investigators and authenticate evidence (protecting its integrity), as well as to protect the confidentiality of the evidence through PKI-based encryption.

4.9.4 Preserving chain of custody

All legal requirements should be complied with and all processes should be properly documented to preserve the chain of custody seeing that the evidence is handled by several different parties. This process is to be performed from the *incident detection* process through until the last process.

4.9.5 Preserving digital evidence

Preserving the evidence means to preserve the integrity of the original digital evidence. In order to achieve this, one must conform to strict procedures from the time that the incident is detected until such time as the investigation is closed. Preservation procedures must ensure that the original evidence is not changed and, even more important, they must guarantee that no opportunity arises during which the original evidence may be changed. The *preserving digital evidence* process should also include assessing and documenting the integrity of digital evidence after the processing of the evidence. For example, after transporting the evidence or after performing analyses on it, the integrity of the evidence should be confirmed [48].

4.9.6 Interaction with the physical investigation

Note that the digital forensic investigation process can be dependent on and interconnected with the physical investigation if such an investigation is conducted in relation to the same incident. Therefore, this activity must define the relationship between the digital forensic investigation process and the physical investigation. Such interaction is important for

preserving the chain of custody, preserving the integrity of the digital evidence, protecting the digital evidence from damage and ensuring an efficient investigation.

Table 4.1 provides a summary of digital forensic principles included in the models that were analysed during this research. Note that some of the models only include principles, while others have descriptions of activities that must be performed to apply the principles, and some even translate principles into processes or sets of processes. Based on related work, the author quoted concludes that there are significant disparities among existing digital forensic investigation processes with regard to digital forensic principles and their incorporation in the models. The author came to the following conclusions:

- Three of the principles detected in the analysed models (*preserving chain of custody*, *preserving digital evidence* and *documentation*) are present – only as principles – in all of the analysed models.
- The other three principles identified (*interaction with the physical investigation*, *managing information flow* and *obtaining authorisation*) are present in only three of the analysed models. In addition, they have been introduced in disparate ways, i.e. either as principles, as a description of activities or as processes within the model.

Disparities that were identified in the existing models show that there is low level of harmonisation in regards to digital forensic principles and its application. This can lead to consequences, especially in cases of cross-border and cross-jurisdiction digital forensic investigations. Consequences can include, but are not limited to:

- Legal and procedural issues and errors can occur if proper authorisations are not in place for each action within the investigation. For example, when performing an internal digital forensic investigation on behalf of a company, one must ensure that the company's legal representative or authorised person gives authorisation for any action taken on the company's information systems. Potentially, system users might also need to give authorisation if their personal data is being accessed. If this is not observed it can lead to violation of the company's policies or even applicable laws, such as privacy law.

- Issues with evidence integrity and process integrity can occur if documentation is not performed properly for each action within the investigation. For example, if examination, analysis and interpretation of digital evidence are not properly documented, the results of digital forensic investigations can be questioned.
- Issues with efficiency, effectiveness and privacy can occur if information flow is not defined. As in every activity, where multiple persons and entities are involved, it is of crucial importance for the efficiency and effectiveness of the digital forensic investigation, to have defined information flows, which will promote collaboration and information sharing. Also, this should prevent dissemination of information to unauthorised users and preserving confidentiality and integrity of information. For example, if two different persons, or even different organisations, are performing *examination and analysis* and *interpretation* processes within the digital forensic investigation, then there must be a defined information flow between these two in order for them to be able to exchange relevant information. If such an information flow is not defined the investigation cannot successfully proceed, or there might be issues with confidentiality, integrity and privacy of exchanged information.
- Integrity and admissibility of digital evidence can be in question if processes of *preserving digital evidence* and *preserving chain of evidence* are not observed throughout the investigation. If at any step of investigation these are not strictly observed, digital evidence and complete results of the investigation might be in question. For example, if during *potential digital evidence storage* process one does not perform *preserving chain of evidence* process constantly, in the form of, for example, chain of evidence log, the integrity of digital evidence can be questioned.
- Potential digital evidence may be lost or corrupted if proper coordination with the physical investigation does not exist. If the physical investigation of the crime scene takes place before the digital forensic investigation, digital evidence can be lost or corrupted. For example, this would happen in case investigators performing a physical investigation switch off computers, it would prevent any live forensic investigation from taking place.

- Errors and omissions can occur when implementing any of the above principles as there exist no harmonised and internationally-accepted guidelines for the implementation of these principles.

Considering the above, it is clear that harmonisation is required for digital forensics principles and also for ways in which these should be applied in the digital forensic investigation process model.

The following section presents the complete schema of the proposed digital forensic investigation process model to allow the reader to gain a better understanding of the model and relations between different processes.

Table 4.1 Overview of the digital forensics principles within related work models

The proposed model		Palmer [39]	Reith et al. [40]	DOJ [41]	Carrier and Spafford [42]	Mandia et al. [43]	Beebe and Clark [44]	Cuardhuáin [45]	Cohen [47]	Casey and Rose [46]	ACPO [51]
Digital Forensics Principles											
1.	Interaction with physical investigation				† (3. Physical crime scene investigation group of phases)						Present as principle and set of processes, including preservation of physical evidence and interviews
2.	Preserving chain of custody	*	*	*	*	*	*	*	*	*	*
3.	Preserving digital evidence	*	*	*	*	*	*	*	*	*	*
4.	Information flow							Described			Partially described
5.	Documentation	*	*	*	*	*	*	*	*	*	*
6.	Obtaining authorisation				† (2. Confirmation and authorisation process)			† (2. Authorisation)			*

Table key:

† Present as process (description of a specific process that relates to a specific digital forensics principle)

* Present as principle

4.10 Digital forensic investigation process model schema

Figure 4.7 represents the entire digital forensic investigation process and allows the reader to view the digital forensic investigation process in its totality. Note that not all concurrent processes run concurrently with all other processes. For instance, *preserving chain of custody* and *preserving evidence* concurrent processes start only with the *implementing pre-incident collection, storage and handling of data representing potential digital evidence* process. However, these processes are not performed during the *assessment process group* in the *readiness class* of processes. Also, the *interaction with physical investigation* process starts only with the *first response* process.

The digital forensic investigation processes are iterative, which implies that after the last process one can return to a previous process. Note, however, that iteration is optional and that one can only return to certain processes (see **Figure 4.7**), namely: *planning* process, *preparation* process, *incident scene documentation* process, *potential digital evidence identification* process, *digital evidence collection* process, *digital evidence examination and analysis* process, *digital evidence interpretation* process, *reporting* process and *presentation* process.

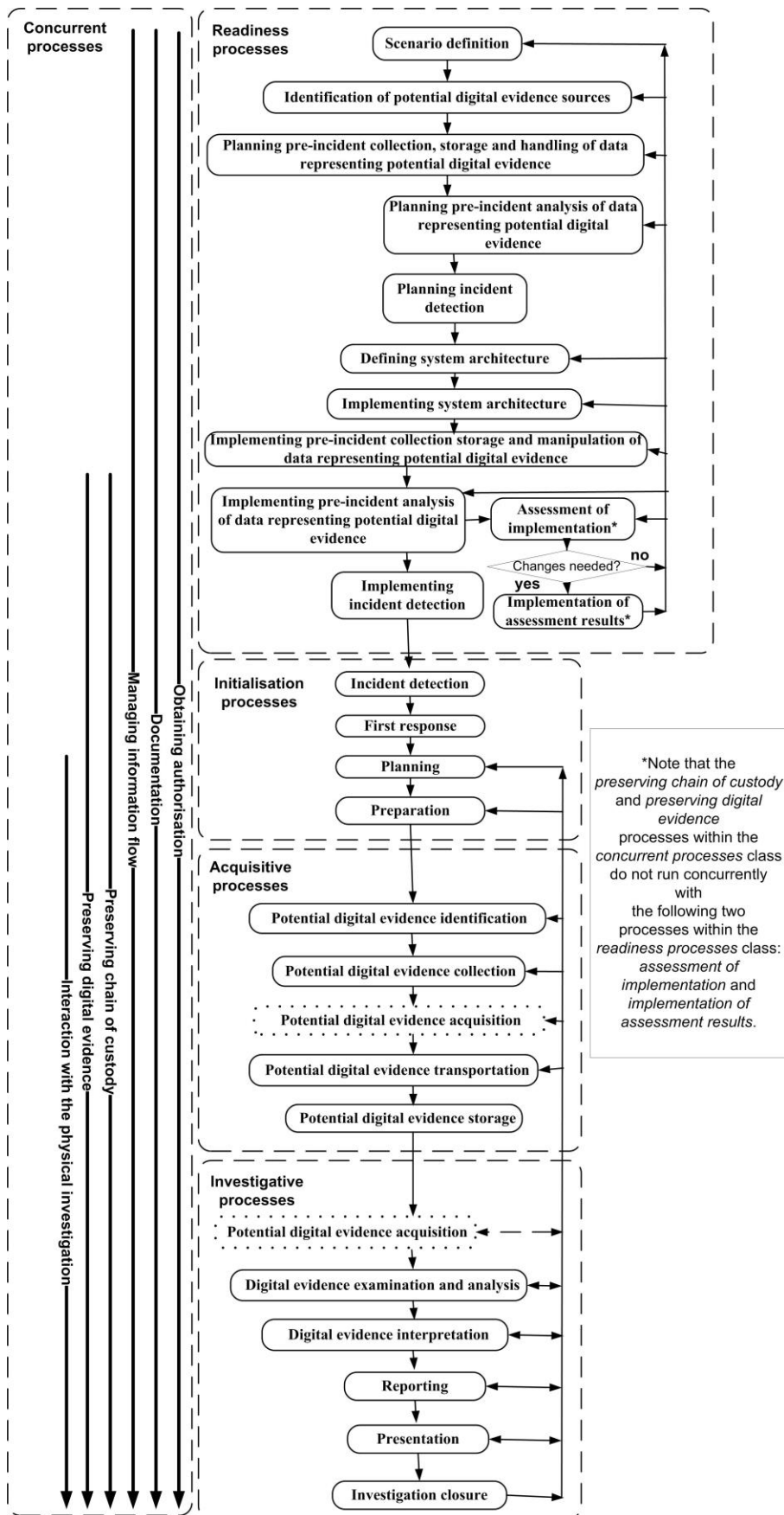


Figure 4.7 Comprehensive harmonised digital forensic investigation process

4.11 Conclusion

In this chapter the author proposed a comprehensive and harmonised digital forensic investigation process model that incorporates *readiness*, *initialisation*, *acquisition* and *investigative* processes, as well as *concurrent* processes. It is important to note that *readiness* processes have been integrated into the proposed model as one of its core parts, thus enabling a comprehensive approach and achieving the greater effectiveness of potential investigations. Implementation of readiness processes is, however, optional within the model, as it will not always be feasible for organisations to implement such a proactive approach, depending on their internal policies, available and needed resources, and specific organisational circumstances. Furthermore, legal systems within certain jurisdictions might or might not enforce some level of implementation of digital forensic readiness processes within specific types of organisations. For example, policy decisions may compel organisations dealing with personal identifiable information (i.e. health service providers, banking organisations, etc.) to implement digital forensic readiness. The rest of the process classes can be implemented, as described in the proposed mode, even if readiness processes have not been implemented.

One of the important novelties introduced is that of a novel class of processes, namely *concurrent* processes, which are aimed at translating digital forensic investigation principles and basic requirements into concrete actions to be taken, in order to ensure investigation effectiveness and the admissibility of digital evidence and the results of the investigation.

The proposed model is a high-level, “umbrella” model, intended to be used across different types of digital forensic investigation. In other words, it is an overarching model covering all aspects and processes of digital forensic investigation. The proposed model gives high-level guidelines and descriptions of the processes comprising the model, its relations, inputs, outputs and importance. Motivation is also given for including specific processes.

The author claims that the proposed model is comprehensive and that it harmonises existing models that were analysed. It must also be noted that the proposed model introduces a range of new benefits and novel approaches such as *concurrent processes* and a comprehensive class of *readiness processes*.

The following chapter provides a comparison of existing models and discusses the benefits of the proposed model when compared to existing models.

CHAPTER 5- COMPARING EXISTING MODELS WITH THE HARMONISED MODEL

5.1 Introduction

After defining the proposed model, the author compared it with existing models to better explain the proposed model's comprehensiveness and added benefits. This is important for understanding particular contributions and benefits allowed by the work of the author. In this chapter the proposed comprehensive and harmonised process model is mapped to existing models, based on the processes (phases) of each of the models studied. The comparison results are summarised in table format (see **Table 5.1**) for ease of viewing.

5.2 Discussion of the comparison

In this section the author first presents a table that summarises the comparison between the proposed model and existing models. Based on the comparison made in **Table 5.1**, the author claims that the model is comprehensive and that it harmonises the existing models (to be discussed later). Each mapped process in **Table 5.1** starts with a number that marks a sequence of processes within the model with which a comparison is being made.

Table 5.1 Comparison of existing models with the proposed harmonised model

	The proposed model	Palmer [39]	Reith et al. [40]	DOJ [41]	Carrier and Spafford [42]	Mandia et al. [43]	Beebe and Clark [44]	Cuardhuáin [45]	Cohen [47]	Casey and Rose [46]	ACPO [51]
Processes											
1.	Incident detection	1. Identification	1. Identification		2. Detection and notification	2. Detection of the incident 3. Initial response	2. Incident response	1. Awareness			
2.	First response					3. Initial response	2. Incident response				2.1 Secure and control the crime scene
3.	Planning		3. Approach strategy		1. Readiness group of processes	4. Response strategy formulation		3. Planning			1. Preparations for investigation
4.	Preparation		2. Preparation	1. Preparation	1. Readiness group of processes	1. Pre-incident preparation	1. Preparation				1. Preparations for investigation
5.	Incident scene documentation			3. Documentation of the crime scene	4.3 Document evidence and scene						2.1 Photograph and document the scene 2.4 Attach exhibit labels

Table 5.1 Comparison of existing models with the proposed harmonised model (continued)

	The proposed model	Palmer [39]	Reith et al. [40]	DOJ [41]	Carrier and Spafford [42]	Mandia et al. [43]	Beebe and Clark [44]	Cuardhuáin [45]	Cohen [47]	Casey and Rose [46]	ACPO [51]
Processes											
6.	Potential digital evidence identification		6. Examination	2. Recognition and identification	4.2 Survey for digital evidence			5. Search for and identify evidence	1. Identification	1. Gather information and make observations	5.1 The collection process
7.	Digital evidence collection	2. Preservation 3. Collection	4. Preservation 5. Collection	4. Collection and preservation	4.1 Preservation of digital crime scene	5. Duplication 7. Secure measure implementation 8. Network monitoring	3. Data collection	6. Collection of evidence	2. Collection 3. Preservation	1. Gather information and make observations,	2.3 Initial collecting of volatile data 5.1 The collection process
8.	Digital evidence transportation			5. Packaging and transportation				7. Transport of evidence	4. Transportation		3. Transport
9.	Evidence storage							8. Storage of evidence	5. Storage		4. Storage
10.	Digital evidence analysis	4. Examination 5. Analysis	7. Analysis	6. Examination 7. Analysis	4.4 Search for digital evidence	6. Investigation	4. Data analysis	9. Examination of evidence	6. Analysis		5.2 The analysis process

Table 5.1 Comparison of existing models with the proposed harmonised model (continued)

	The proposed model	Palmer [39]	Reith et al. [40]	DOJ [41]	Carrier and Spafford [42]	Mandia et al. [43]	Beebe and Clark [44]	Cuardhuáin [45]	Cohen [47]	Casey and Rose [46]	ACPO [51]
Processes											
11.	Digital evidence interpretation				4.5 Digital crime scene reconstruction			10. Hypothesis	7. Interpretation 8. Attribution 9. Reconstruction	2. Form hypothesis to explain observations 3. Evaluate the hypothesis 4. Draw conclusions and communicate findings	5.3 The examination process
12.	Reporting			8. Report		10. Reporting					5.4 The reporting process
13.	Presentation	6. Presentation	8. Presentation	8. Report	4.6 Presentation of digital scene theory	10. Reporting	5. Findings presentation	11. Presentation of hypothesis 12. Proof/Defence of hypothesis	10. Presentation	4. Draw conclusions and communicate findings	5.4 The reporting process
14.	Investigation closure	7. Decision	9. Returning evidence			9. Recovery 11. Follow-up	6. Closure	13. Dissemination of information	11. Destruction		6. Disclosure

Table 5.1 Comparison of existing models with the proposed harmonised model (continued)

	The proposed model	Palmer [39]	Reith et al. [40]	DOJ [41]	Carrier and Spafford [42]	Mandia et al. [43]	Beebe and Clark [44]	Cuardhuáin [45]	Cohen [47]	Casey and Rose [46]	ACPO [51]
Concurrent processes											
1.	Interaction with physical investigation				† (3. Physical crime scene investigation group of phases)						Present as principle and set of processes, including preservation of physical evidence and interviews
2.	Preserving chain of custody	*	*	*	*	*	*	*	*	*	*
3.	Preserving digital evidence	*	*	*	*	*	*	*	*	*	*
4.	Information flow							Described			Partially described
5.	Documentation	*	*	*	*	*	*	*	*	*	*
6.	Obtaining authorisation				† (2. Confirmation and authorisation process)			† (2. Authorisation)			*

Table Key:

* Present as principle

† Present as process (description of a specific process that relates to a specific digital forensics principle)

As is evident from **Table 5.1**, none of the existing models covers all the processes included in the proposed model and thus the author can claim comprehensiveness of the proposed model. Furthermore, the author included relevant processes from the existing models so as to achieve harmonisation.

The proposed model is iterative and multi-tiered, and one can potentially traverse through a number of iterations. The model clearly defines allowable routes to be followed, as shown in **Figure 4.7** above. For example, from *digital evidence examination and analysis* process one can go back to *identifying potential digital evidence* process and thus start a new iteration. On the other hand, one cannot go back from the *potential digital evidence storage* process to any of the previous processes. The model is composed of several tiers, where process classes represent a higher-level tier and processes represent a lower-level tier. The model also allows for the further division of processes into subprocesses to provide for the development of more specific guidelines for different types of investigations, such as mobile forensics, cloud forensics, live forensics, etc.

The author also introduced *concurrent processes*, as these would ensure higher efficiency and digital evidence admissibility. This is an important contribution and a novel approach to the principles of digital forensics, and it would ensure that these principles are applied consistently throughout the digital forensic investigation. Also, the author included a comprehensive *readiness processes* class to incorporate digital forensic readiness within an organisation before the investigation takes place (if applicable).

Note also that the order of the processes differs from some of the previous models and that the author believes that the proposed order makes provision for a more efficient investigation process.

As stated above, the author proposes a number of processes aimed at achieving digital forensic investigation readiness. These are not shown in the comparison table above, as the analysed models mostly did not include structured digital forensic investigation readiness processes. There are two exceptions. Mandia et al. [43] proposed a single readiness oriented process. The second exception is the work done by Carrier and Spafford [42], which included a readiness processes group. This group includes two processes (phases), namely an operations readiness phase and an infrastructure readiness phase. The operations readiness phase is aimed at providing the right personnel and equipment needed for a potential digital

forensic investigation. The infrastructure readiness phase is intended to ensure that the data needed to perform the investigation exists and is oriented towards introducing specific technological solutions or actions for this purpose (e.g. introducing video cameras or performing hash functions).

Table 5.2 presents a comparison between the readiness processes class within the proposed model and that encountered in related work.

Table 5.2 Comparison of the readiness processes class in the proposed model with readiness processes found in related work

	The proposed model-readiness processes	Tan [27]	Carrier and Spafford [42]	Rowlingson [65]
1.	Scenario definition			Define the business scenarios that require digital evidence
2.	Identification of potential digital evidence sources	What is logged	Infrastructure readiness	Identify available sources and different types of potential evidence
3.	Planning pre-incident collection, storage and handling of data representing potential digital evidence	How logging is done Digital forensic acquisition	Operations readiness Infrastructure readiness	Determine the evidence collection requirement Establish a capability for securely gathering legally admissible evidence to meet the requirement Establish a policy for secure storage and handling of potential evidence
4.	Planning pre-incident analysis of data representing potential digital evidence	Intrusion detection systems		Ensure monitoring is targeted to detect and deter major incidents
5.	Planning incident detection	Intrusion detection systems		Specify circumstances when escalation to a full investigation should be launched
6.	Defining system architecture			

Table 5.2 Comparing the readiness processes class in the proposed model with readiness processes found in related work (continued)

	The proposed model-readiness processes	Tan [27]	Carrier and Spafford [42]	Rowlingson [65]
7.	Implementing system architecture			
8.	Implementing pre-incident collection, storage and handling of data representing potential digital evidence	How logging is done Digital forensic acquisition	Operations readiness Infrastructure readiness	Determine the evidence collection requirement Establish a capability for securely gathering legally admissible evidence to meet the requirement Establish a policy for secure storage and handling of potential evidence
9.	Implementing pre-incident analysis of data representing potential digital evidence	Intrusion detection systems		Ensure monitoring is targeted to detect and deter major incidents
10.	Assessment of implementation			
11.	Implementation of assessment results			
12.	Implementing incident detection	Intrusion detection systems		Specify circumstances when escalation to a full investigation should be launched Document an evidence-based case describing the incident and its impact

First it can be concluded that readiness processes present in related work are quite disparate in terms of scope and level of guidance provided.

The processes in the *readiness processes* class of the proposed model have a wider scope when compared to existing models. This wider scope is especially manifested through the following three additional processes as defined in the proposed model, namely *pre-incident data analysis* process, *architecture-definition* process and *assessment* process – none of which is included in existing models. Furthermore, the author included *defining system architecture* process, to be applied to the target information system to achieve the aims of digital forensic readiness for that information system. Introducing a customisation of architecture of the information system as part of achieving digital forensic readiness for that system constitutes a novel approach to the matter. The author believes it is a very important contribution as it allows for a more holistic approach to digital forensic readiness and a more efficient proactive approach to digital forensic investigations. Those processes that already exist in other models now have a much wider scope and are better defined in the proposed model.

The author also defined the following aims for a *readiness processes* class, which are harmonised mostly from previous work [24, 42, 43, 44, 48, 63-65], except for the last aim that was added by the author and is a novel and important contribution. The processes in this class should achieve the following:

1. Maximise the potential use of digital evidence
2. Minimise the costs of digital forensic investigations incurred
3. Minimise interference with and prevent interruption of business processes
4. Preserve or improve the current level of information security

The author firmly believes that the last aim listed above should be taken into account. This is a novel aspect and a contribution aimed at adopting a more holistic approach towards the matter of achieving digital forensic readiness from the perspective of information systems security.

In order to further stress the uniqueness and comprehensiveness of the proposed model, the author now makes a comparison between the proposed model and existing models with regard to the number of processes included in the model.

Table 5.3 Number of processes present in the analysed models

Model	Number of processes
The proposed model	32
Palmer [39]	7
Reith et al.[40]	9
DOJ [41]	7
Carrier and Spafford [42]	17
Mandia et al. [43]	10
Beebe and Clark [44]	6
Cuardhuáin [45]	13
Cohen [47]	4
Casey and Rose [46]	11
ACPO [51]	15

As can be seen from **Table 5.3**, the proposed model has a significantly higher number of proposed processes, which further shows its comprehensiveness. It is important to note that the higher number of processes in the proposed model is not the result of dividing existing processes into sub-processes, but rather because of the introduction of the comprehensive *readiness processes* class and the novel *concurrent processes* class. They also encompass all relevant processes proposed by the existing models.

In order to emphasise the uniqueness of the proposed model when compared to existing models, the author also compared these based on the following qualitative characteristics:

- Width of the area of concentration
- Granularity of the area of concentration
- Level of detail
- Area of application
- Technology oriented or process oriented?

The author next gives an explanation of each of the characteristics above.

- Width of the area of concentration

‘Area of concentration’ defines the main area of concentration for the specific model. The areas are defined as a specific process or group of processes (for example incident response, or analysis and interpretation that are included in the proposed model). ‘Width of the area of concentration’ of the model is a qualitative measurement that defines how many of the relevant process groups have been included in the model. 0 is assigned for a narrow area of concentration (covering a few specific areas of processes such as first response or investigative processes) and 1 for a wide area of concentration (covering all areas of the digital forensic investigation process). Values between 0 and 1 are qualitative determinations by the author with regard to the width of the area of concentration of analysed models. Keep in mind that a value of 1 or close to 1 does not necessarily mean the model in question is comprehensive, but rather that it covers the full width of relevant process groups, while not necessarily including all relevant and needed processes within that group.

- Granularity of the area of concentration

Granularity of the area of concentration of the model is a qualitative measurement that defines how many of the relevant processes have been included in the model. 0 is assigned for less granular area of concentration (covering a few specific processes) and 1 for deep area of concentration (covering all relevant process). Values between 0

and 1 are quantitative determinations based on the number of processes that exist in the analysed model. The value is calculated as number of processes present, divided by 32, which is the number of processes in the proposed model, rounded to one decimal place. This parameter, in combination with the previous parameter, is a good measure of the comprehensiveness of the specific model.

- Level of detail

This characteristic defines the level of detail that is present in a specific model. The level of detail can be high, if high-level guidance and framework are provided or when principles are defined and presented. On the other hand, the detail can be of a lower level, if it provides detailed and specific guidelines, processes, tools, methods or techniques.

- Area of application

This characteristic defines the intended, prescribed or envisaged application area of the specific model. The area of application can for example be criminal investigations, civil investigations or enterprise investigations.

- Technology oriented or process oriented?

This characteristic defines if the specific model is oriented towards processes or towards technology. Usually, high-level models such as the model proposed in this thesis will be process oriented, while low-level models will be technology oriented and will provide more technology-related details. Process-oriented models are often technology neutral and do not favour or prescribe a certain technology or a certain technological solution. On the other hand, technology-oriented models prescribe (though most often not mandatory) specific technological solutions to be applied.

The comparison summary is presented in **Table 5.4**.

Table 5.4 Characteristics of the analysed models

Model	Width of the area of concentration	Granularity of area of concentration	Level of detail	Area of application	Technology oriented or process oriented?
The proposed model	1	1	High	Civil, criminal and enterprise investigations	Process oriented
Palmer [39]	0.7	0.2	High	Civil, criminal and enterprise investigations	Process oriented
Reith et al. [40]	0.7	0.3	High	Civil, criminal and enterprise investigations	Process oriented
DOJ [41]	0.7	0.2	Low	Criminal investigations	Process and technology oriented
Carrier and Spafford [42]	0.9	0.5	High	Civil, criminal and enterprise investigations	Process oriented
Mandia et al. [43]	0.9	0.3	High	Civil, criminal and enterprise investigations	Process oriented
Beebe and Clark [44]	1	0.2	High	Civil, criminal and enterprise investigations	Process oriented
Cuardhuáin [45]	0.8	0.4	High	Civil, criminal and enterprise investigations	Process oriented
Cohen [47]	0.7	0.1	High	Civil, criminal and enterprise investigations	Process and technology oriented
Casey and Rose [46]	0.6	0.3	High	Civil, criminal and enterprise investigations	Process oriented
ACPO [51]	0.8	0.5	Low	Criminal investigations	Technology oriented

It is clear from the comparison in **Table 5.4** that the proposed model is comprehensive and unique, especially in terms of depth of the area of concentration. Existing models have a good width of area of concentration, and especially the three models proposed in [42-44], but they lack the level of granularity offered by the proposed model. It is worthy to note that the models presented in Government-issued guidelines are more technology oriented, contain more low-level detail and are primarily intended for use in criminal digital forensic investigations.

The author now gives a graphical presentation (**Figure 5.1**) of the comparison in terms of width of the area (model’s width) of concentration and granularity of the area of concentration (model’s granularity) with the view to providing a visualisation of the comprehensiveness of the proposed model.

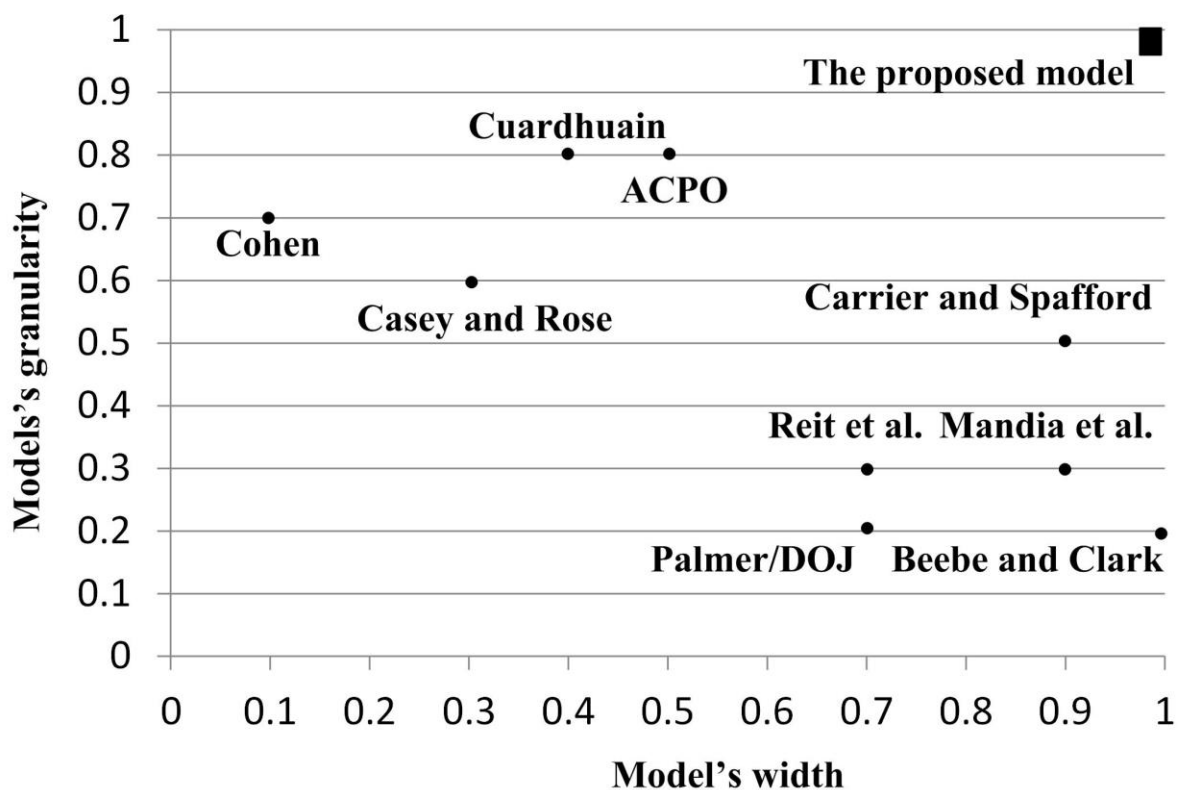


Figure 5.1 Comparing the proposed model with the existing models

The followings section concludes the chapter.

5.3 Conclusion

In **Chapter 5** the author compared the proposed model to existing models that were used as a starting point for construction of the proposed model. The comparison is shown in the form of a table that clearly illustrates the level of comprehensiveness and harmonisation achieved. The comparison and specific novelties and contributions of the proposed model were subsequently discussed.

Chapter 6 explains the testing that was performed to evaluate the proposed process model. Testing was conducted in the form of an analysis of the implementation of the proposed process model to solve real-world cases. In this way, the proposed model was evaluated in terms of usability, adaptability, effectiveness, benefits and flaws.

CHAPTER 6- ANALYSIS OF THE RESULTS OF IMPLEMENTING THE PROPOSED PROCESS MODEL

6.1 Introduction

In this chapter the author analyses the results obtained through implementation of the proposed process model in real-world cases in order to evaluate the usability and effectiveness of the proposed process model.

Testing was performed by the author and fellow researchers from the ICSA (Information and Computer Security Architecture) research group of the Computer Science Department at the University of Pretoria. The conclusions of such testing were published in relevant papers [72, 74, 75] published over the past two years. In order to complete this task, ICSA collaborated with a digital forensic investigations private company (to remain anonymous), who provided their equipment, software and advice needed to perform digital forensic investigations.

Out of numerous test cases, three representative cases are reported on in the subsections that follow. These cases involved different types of digital forensic investigations, and two were mobile forensic investigations (one on Android platform [76] and one on BlackBerry platform [77]), while the third was a post-mortem forensic investigation. (For more background information on the different types of digital forensic investigation, please refer to the *Background* chapter.)

Each of the three cases is discussed in more detail in the sections to follow and the structure of each discussion is as follows: For each of the presented cases, the testing methodology is explained first; next the case scenario is presented, followed by findings and observations.

In the first of the three representative cases, the author gives a detailed overview of implemented processes within the proposed model, so that the reader can fully appreciate how the model was implemented.

6.2 Case 1 - Mobile digital forensic investigation into a case of intellectual property theft

6.2.1 Methodology

The testing of the proposed process model was carried out with commercial mobile forensics software of the Micro Systemation XRY V6.5 Mobile Forensic toolkit [73].

In the *preparation* process, the following equipment was needed [72]: the XRY complete toolkit for mobile device examinations; an XRY licence key USB stick; a write blocker; a forensically cleaned USB drive; a desktop PC with Windows OS 8; a Subscriber Identity Module (SIM) adapter; a forensically cleaned hard drive; and an empty Digital Video Disc (DVD). A Faraday bag was used to package and isolate the mobile device from the network during a *potential digital evidence collection* process, while a digital camera was used to document the potential evidence and crime scene.

The case included mobile forensic activities for a BlackBerry [77] mobile device as will be explained below.

6.2.2 Case scenario

In this case study [72], Company XYZ holds the intellectual property rights for the advertising concepts developed by their creative team. Non-compete agreements are in place to deter an employee from stealing intellectual property from an employer and creating a competing entity using the former employer's concepts.

Company XYZ learnt of the formation of a competing company by its former employees. The head of human resources of Company XYZ contacted digital forensic investigators (Investigator ABC) as they believed that communications regarding the new venture had taken place on a company asset (a BlackBerry [77] mobile device) formerly used by the employee involved. To confirm this suspicion, Investigator ABC was instructed to carry out a digital forensic investigation on the said mobile phone.

Investigator ABC found that cases involving the infringement of a non-compete agreement and the theft of intellectual property mostly involve former employees using company assets such as laptops or a smartphone, as was suspected in this case, to correspond with co-conspirators. It was suspected that the digital evidence might still be present on the particular

phone in the form of text messages, but that such messages might possibly have been deleted. Despite the possible deletion of the data, an experienced digital forensics expert can in most cases recover the deleted data.

The investigation was successful and the results obtained during the *interpretation* process of the investigation confirmed that the former employee of Company XYZ indeed used the mobile device for stealing intellectual property with the aim to create a competing entity. Company XYZ received all the necessary reports and information during the investigation closure process, after which they could use these to prosecute the perpetrator.

The next subsection gives more details on processes performed during the implementation of the proposed model.

6.2.3 Details on the performed processes

The following subsections explain in detail the implementation of the process in the case at issue [72].

a) Incident detection process

The incident was detected by an Employee of Company XYZ, who noted the creation of a competing entity. Company XYZ further enquired and discovered that one of the founders of this competing company had been a former employee of Company XYZ. The company reported the incident to top management, who contacted Investigator ABC to conduct a digital forensic investigation, as it was suspected that the information security incident led to unfair competition by the newly established company.

b) First response process

The *first response* process involves measures taken by the first responder. In this case the first responder ensured that the mobile device was isolated from the network to prevent incoming calls and messages that could potentially alter the potential evidence residing on the mobile device. The first responder from Company XYZ contacted Investigator XYZ to collect the mobile device.

c) *Planning process*

During this process, the company provided the investigators with a description of the case to be investigated, and the investigators documented all required resources and equipment. The resources and equipment were listed in the process to follow, specifically to suit a mobile forensic investigation. The investigators obtained authorisation from Company XYZ to extract potential digital evidence from the mobile device.

d) *Preparation process*

During the preparation process, the investigators prepared all the required equipment, ranging from hardware to software tools. The resources and equipment for this particular case included the XRY complete package (Micro Systemation), which comprises the XRY application software and licence key, write-protected universal memory card reader, Windows OS 7 [78], a Subscriber Identity Module (SIM) [79] identity cloner, XRY complete mobile phone cable kit and XRY communication unit. Other resources that were required included a DVD used to provide a copy of the potential evidence to the various stakeholders. A desktop computer running the Windows OS 7 [78] operating system was also prepared. A Faraday bag was used to isolate the mobile device from the network during the *potential digital evidence collection and preservation* process. A digital camera was also provided to later document the potential evidence and crime scene.

e) *Potential digital evidence identification process*

During this process, the investigators identified the potential evidence that could be located on the mobile device; hence the mobile device was the potential source of digital evidence. In this scenario, it was quite obvious that this device contained the potential digital evidence. However, in different scenarios there might be more sources of potential digital evidence as well as latent potential digital evidence, for instance personal computers, external hard drives, etc.

The investigators identified the potential evidence and documented the details of the mobile device as a BlackBerry 9300 Curve [80]. Identification of digital evidence included an examination of the device for any physical damage and the documentation of all identifying details such as the model and serial number (i.e. International Mobile Equipment Identity

(IMEI) number). The investigators also documented information related to date and time zone.

f) Potential digital evidence collection process

During the collection of the potential digital evidence, the mobile device was collected as the source of potential evidence and clearly labelled and placed in a Faraday bag as part of the *documentation and preserving digital evidence* concurrent processes, which will be discussed later. This process was also assisted by maintaining the chain of custody and information flow.

g) Potential digital evidence transportation process

During the transportation of digital evidence, the mobile device was physically transported to a laboratory in a secure and forensically sound manner. The chain of custody was observed and followed during such transportation.

h) Potential digital evidence storage and preservation process

Digital evidence needs to be stored if an analysis cannot be conducted immediately. The digital evidence (the mobile device itself) was stored in a secured locker. The chain of custody and preservation of the integrity of evidence was maintained by ensuring that an evidence ledger (chain of custody) was kept to keep trace of evidence.

i) Potential digital evidence acquisition process

During *potential digital evidence acquisition* process a copy of each of any potential digital evidence source was produced and the potential digital evidence is extracted from the following sources: internal memory of the mobile device, SIM card memory, and Secure Digital (SD) memory.

Potential evidence was extracted from the mobile device by using the XRY extractor tool. The mobile device was connected to a desktop computer using a cable for the acquisition of all the data residing on the mobile device. A logical acquisition was conducted on the internal memory of the mobile device and the retrieved data comprised the type of operating system, make, model of the mobile device, web bookmarks, contacts, SMS (Short Message Service)

messages, pictures, audio, video, documents, MMS (Multimedia Message Service) messages, email, calendar, tasks, and notes.

Next, the investigators also conducted a logical acquisition on the SIM card and extracted potential evidence from the SIM card by cloning the original SIM card. The investigators used a SIM cloner to create a duplicate SIM card that contained the critical data residing on the original SIM card and was designed to isolate the mobile phone from the mobile network. This practice is very similar to using a write blocker when acquiring data from a hard drive. The investigators subsequently placed this specially cloned SIM card into the mobile device so as to avoid any further update or changes to the potential evidence that resided on the mobile device. Potential evidence extracted from the cloned SIM card included the Network code from the International Mobile Subscriber Identity (IMSI), mobile number, contacts on the SIM card, and SMS messages on the card. The cloned SIM cards hold two essential identities that were retrieved during this process, namely the Integrated Circuit Card Identifier (ICCID) and IMSI.

The potential evidence from the SD memory card was acquired using a physical acquisition, thus creating a bit-for-bit copy of an entire physical store. The use of logical and physical acquisition allows for the recovery of any deleted data that once resided on the memory SD card. In this case, such data consisted of contacts, MMS messages and files (pictures, music, documents, sound clips, and videos).

The investigators adhered to all legal requirements during this process while seeking consultation from relevant guidelines and international standards.

j) Digital evidence examination and analysis process

During the *digital evidence examination and analysis* process, the investigators examined the data acquired from the digital evidence and analysed the potential evidence recovered from the mobile device's various memory acquisitions. The examination and analysis techniques of the potential evidence used by the investigators included timeframe construction, extraction of hidden data, extraction of application files and ownership details. This process was used to determine the significance of the digital evidence extracted from the mobile device in this specific case study. The significance was determined by grouping the potential evidence according to the file format of such documents, emails, and SMSs.

Based on the examination and analysis that was performed the investigators have set up a hypothesis on the course of events relating to the incident.

The investigators documented each and every step in a forensically sound manner by carefully adhering to the prescriptions of the proposed model. Due to the volatile nature of the mobile device, the investigators ensured that the potential source of digital evidence was handled with critical care to make certain that the mobile device remained isolated from the network to avoid any change to the data residing on it. The investigators took into account the physical state of the potential source of evidence by conducting a physical inspection of the mobile device.

k) Digital evidence interpretation process

The interpretation of the digital evidence extracted from the mobile device proved to be of great significance. The investigators categorised the evidence according to the significance of the case and concentrated on the potential evidence extracted from the mobile device. The evidence of interest included emails, documents, contacts, and SMS messages, which were first priority in the case, as these may have been used as main means of communication. During the *digital evidence interpretation* process, the investigators narrowed down the significant data within certain documents, call logs, SMS messages and MMS messages that were of importance to this case. The data which was identified as significant was used to prove the hypothesis from the previous process.

l) Reporting process

The results obtained from the *digital evidence interpretation* process showed that the former employee of Company XYZ used the mobile device to steal intellectual property with the aim of creating a competing entity. The investigators compiled a report detailing all the processes and all the different techniques used during the investigation, as suggested by the proposed model. Relevant information concerning the process that was followed, the extraction methods, tools, and techniques used were clearly stated in the report. The investigators' interaction with the potential evidence was elaborated on in the report in a forensically sound manner, hence confirming accountability and integrity. The investigators presented the report to all the relevant stakeholders involved in this particular case.

m) Presentation process

The investigators presented the findings based on the digital evidence analysed during the *digital evidence interpretation* process in the form of expert report to the various stakeholders. The report contained evidence that proved a violation of the non-compete agreements in the form of emails and SMS messages.

During the *presentation* process, the investigators confirmed that all the processes as defined in the proposed model and in ISO/IEC 27043:2015 [21] were used to verify that the investigation was conducted in a forensically sound manner. A detailed report was subsequently compiled by the investigators involved in the investigation.

n) Investigation closure process

The investigation was closed after presentation of the report. Thereafter, the mobile device and potential digital evidence collected during the investigation were returned to Company XYZ. These findings could then be used in a prosecution case at the discretion of Company XYZ against their former employee.

The following subsection explains the findings and observations from this case in regards to the implementation of the proposed prototype.

6.2.4 Findings and observations

The following findings and observations were made [72]:

- Since the proposed model worked effectively for a mobile digital forensic investigation, it could be assumed that the proposed model would be applicable to other mobile devices as it is a generic process model.
- In order to ensure full performance of the process model, investigators with adequate knowledge and skills are required to produce reliable and admissible potential digital evidence.
- The *documentation* process has proved to be vital during the testing.

- The investigators should always prepare for their case according to the type of digital forensic investigation, as this preserves not only the integrity of the potential evidence, but also the creditability of the investigators conducting the investigation.
- During the investigation, the model displayed effectiveness as well as flexibility, adaptability, integrity, comprehensiveness, and accountability.
- The *concurrent processes* were fully applicable during the testing of the model by ensuring that the investigators followed the proper legal processes and procedures.
- The proposed model is well structured.

An evaluation table was also presented in [72] to map out where each process fulfilled a particular criterion during the mobile forensic investigation. An X was used to mark the applicability of the different criteria to the processes.

Table 6.1 next assists in evaluating the proposed model.

Next the author explains some of the criteria used to evaluate the model in the above-mentioned table. Some examples are given below on how processes fulfilled specific criterion.

The *planning* process displayed flexibility by allowing the investigators to consider the equipment and resources that were required specifically to conduct a mobile forensic investigation. This allowed the incorporation of other related standards and guidelines as the investigation proceeded. A pertinent example could be that of the *potential digital evidence storage* process. The various sources of the potential digital evidence are stored differently and handled according to their size. An example would be a USB device and a mobile phone. The USB device takes up less space and requires less storage precautions.

During the *digital evidence acquisition* process the model demonstrated adaptiveness. For example, data acquisition onsite (being at the incident scene) is different from data acquisition offsite (being in a digital forensics laboratory), where the difference is often manifested through the use of different procedures, methods and tools. The model was developed in a way to allow for the application in different types of digital forensic investigation.

Integrity was illustrated by the implementation of *concurrent processes*, which ensure the integrity of the process and also the integrity of digital evidence. For example, *preserving chain of evidence* and *preserving digital evidence* are aimed directly at preserving the integrity of evidence, while other concurrent processes such as documentation and obtaining authorisation also assist in achieving this aim.

Table 6.1 Model evaluation table [72]

Process	Flexibility	Adaptiveness	Integrity	Comprehensiveness	Effectiveness	Accountability
Incident detection				X		X
First response	X	X	X	X	X	X
Planning	X	X	X	X	X	X
Preparation	X	X	X	X	X	X
Incident scene documentation	X		X		X	X
Potential digital evidence identification	X	X	X	X	X	X
Potential digital evidence acquisition	X	X	X	X	X	X
Potential digital evidence transportation	X	X	X	X	X	X

Table 6.1 Model evaluation table [72] (continued)

Process	Flexibility	Adaptiveness	Integrity	Comprehensiveness	Effectiveness	Accountability
Potential digital evidence storage	X	X	X	X		X
Digital evidence examination and analysis			X	X	X	X
Digital evidence interpretation			X	X		X
Report writing			X	X	X	X
Presentation	X	X	X	X	X	X
Investigation closure	X	X	X	X	X	X

Comprehensiveness was displayed by the majority of the processes of the proposed model as shown in **Table 6.1**. The proposed model and processes are comprehensive and they allow and accommodate all the needed activities within the digital forensic investigation. Not a single activity was performed that was not part of the processes defined in terms of the proposed model.

Effectiveness, linked with skilled personnel and a holistic process model, led to achieving the results of the investigation in reasonable time and without exceeding the planned budget. This is a direct reflection of the fact that a clear understanding of the type of digital forensic investigation often improves results and increases the effectiveness of the *preparation* process. Further, effectiveness of the investigation is enabled by the fact that there are clear guidelines for the complete duration of the investigation, encompassing all relevant activities.

Also, the proposed model includes the *planning* and *preparation* processes that enable one to conduct the investigation effectively. Finally, for the investigation to be effective, digital evidence, which is result of the investigation, has to be admissible in court. The model strongly contributes to this aim, especially through the proposed *concurrent processes*, which ultimately ensure digital evidence integrity and enable one to verify that a reliable and acceptable process was applied throughout the duration of investigation.

Accountability was observed to be applicable throughout all the processes of the proposed model. Through access control, the identification of investigators and examiners who interacted with the potential digital evidence assisted in maintaining a high level of responsibility during the investigation. For example, the examiners are expected to account for the measures and tools used during the *digital evidence analysis* process. The processes are proposed in such a way that for each of the actions there must be appropriate authorisation, thus creating accountability for actions through the *obtaining authorisation* concurrent process. The concurrent processes of *preserving digital evidence*, *preserving chain of evidence* and *documentation* also strengthen the accountability quality of the proposed model.

In the following section the author presents the case of a mobile digital forensic investigation on an Android mobile device.

6.3 Case 2 - Mobile digital forensic investigation with regard to phishing using a scareware attack

6.3.1 Methodology

Testing methodology was the same as for the previous case described.

The proposed process model was tested through its implementation in a real-world case involving a mobile device with an Android operating system. Due to the confidentiality agreements in place and the sensitivity of the case, some of the details presented in the case scenario (**Section 6.3.2**) are withheld or rendered anonymous.

6.3.2 Case scenario

The case analysed [74] involves a phishing attack using scareware, targeted at customers of bank XYZ via SMS. The mobile device targeted with the SMS scareware was a Samsung

mobile Galaxy S2 phone belonging to customer ABC of bank XYZ. The suspect/attacker distributed scareware to bank X clients via SMS and mimicked Bank XYZ by requesting the clients to click on the sent link to update their account details or else lose their data held with the bank. An unsuspecting customer of Bank XYZ fell victim to this phishing attack. After obtaining the victim's details, the suspect performed an unauthorised transaction on the customer's bank account. An alert received by the bank's customer for a transaction that he/she never initiated, raised the customer's suspicion, who then reported the incident to Bank XYZ.

The case was successfully resolved and the perpetrator was identified and charged.

6.3.3 Findings and observations

The following findings and observations were made [74]:

- The proposed process model adequately accommodated the investigation of an Android mobile phone.
- A valuable contribution of the proposed process model was the introduction of *concurrent processes*, which helped to preserve the integrity of the investigation and digital evidence.
- Potential difficulty was identified in that it is very important to have the full cooperation of and a clear understanding between the different personnel involved – which may be hard to achieve. The author would like to emphasise here that concurrent processes of *documentation* and *managing information flow* are intended to solve and prevent such difficulties. The *documentation* concurrent process was also emphasised as particularly important for solving this challenge.
- The proposed process model was found to effectively accommodate the investigation of Android devices, and therefore mobile devices in general, as long as the concurrent processes were strictly implemented from the beginning of an investigation through to its conclusion.

The third and last case discussed in this thesis, as presented in the following section, is a digital forensic post-mortem investigation.

6.4 Case 3 - Digital forensic post-mortem investigation with regard to the contravention of company user policy

6.4.1 Methodology

During the *preparation* process, the investigators prepared all relevant equipment and resources as will be described in **Table 6.2** [75].

Table 6.2 List of resources and equipment prepared for the investigation [75]

Resources (Item)	Purpose of the resources
Two forensically clean drives	Used as a destination to store the imaged hard disk for processing. The second drive is a backup used to store the copy of the imaged hard disk, in case the destination drive is corrupted or compromised.
Tableau TD2 forensic duplicator (2013)	Used for imaging the hard disk without compromising it.
Hardware-based write blocker device	Used to ensure that Windows does not alter the suspect's hard disk when attached to the computer.
A blank DVD	Used to provide a copy of the potential digital evidence obtained during the investigation.
A digital camera	Used to take photographic images of the evidence and crime scene.
A Faraday bag	Used to package potential digital evidence during the digital evidence collection process.
A USB Dongle	Plugged into the investigator's computer to run Access Data FTK in full mode.
Forensic Toolkit (FTK) 3.2 imager	Used to preview recoverable data from a disk, as well as to create perfect copies, called forensic images.
Software products keys	Used to ensure that the software application is genuine.

6.4.2 Case scenario

For the sake of testing and evaluating the model, the scenario used was as follows [75]: Company XYZ suspected one of their employees of using company resources to download pornographic material during office hours. According to its user policy, Company XYZ regards any form of pornography as illegal and unacceptable.

The system administrator detected this incident when he noticed a constant visit to a particular pornographic website from a computer used by a specific employee. He immediately notified the head of the department, who then requested Investigator ABC (who conducts digital forensic investigations) to investigate the allegation.

The investigation was successful. The results obtained from the *interpretation* process showed that the employee of Company XYZ had violated company policy with regard to internet usage. The digital evidence found included photos, documents and videos. Based on reports and information handed to the company, Company XYZ proceeded to make a decision on the case based on the company's policy.

The reader should note that the author does not intend to present here a detailed overview of each action taken within or the full results of this investigation, as that would fall outside the scope of this thesis. Information presented here has the aim to provide the details of a testing case and the findings and observations made by the testers.

6.4.3 Findings and observations

The following findings and observations were made [75]:

- The proposed model was found to be effective and applicable when used during a post-mortem digital investigation.
- The proposed model allowed the investigators to account for every action conducted.
- The *concurrent processes* ensured that each step conducted during the investigation was documented and each interaction was accounted for by clearly adhering to the rules and norms of conducting a forensically sound investigation.
- The *concurrent processes* were adequately adaptable during the post-mortem digital forensic investigation.

- The *concurrent processes* assisted in the preservation of the integrity, confidentiality and availability of the potential evidence.

The following section summarises the results of testing the proposed model in a real-world context.

6.5 Summary of the testing results

Based on the tests performed on three real-world cases as described in the sections above, the results can be summarised as follows:

- The proposed process model adequately accommodates mobile digital forensic investigations and post-mortem digital forensic investigations. As the proposed process model is generic enough, the author firmly believes that the tests performed indicate that the model could easily be applied to other types of digital forensic investigation.
- A valuable contribution of the proposed process model is its introduction of *concurrent processes* that help to preserve the integrity of the investigation and digital evidence as well as to adhere to digital forensic principles. The *concurrent processes* were fully applicable during the testing of the model.
- The proposed model shows qualities of effectiveness, flexibility, adaptability, integrity, comprehensiveness and accountability, based on the criteria discussed in **Section 6.2**.
- Identified challenges can be remedied through strict adherence to the implementation of the processes within the model, and if special attention is paid to *concurrent processes*. There is a need to strictly follow *concurrent processes* so as to establish effective coordination and communication between the different parties involved. This challenge can be solved through the consistent use of the *managing information flows* concurrent process and the *documentation* concurrent process. However, as process guidelines in this thesis are high-level, the author recognised the need for defining the *managing information flow* process in detail for specific investigations and even possibly for it to be supported by specialised management processes and tools.

6.6 Conclusion

This chapter presented results of the implementation of the proposed process model in real-world cases in order to evaluate its usability and effectiveness.

The model was tested on three real-world cases, which were all successfully solved. Two of these cases were mobile forensic cases and one was a dead-forensic case. The testing showed that the proposed model is adaptable and generic enough to be used in different types of investigation. Further implementation of the proposed model helped to achieve effectiveness and enable higher admissibility of digital evidence, especially through the strict implementation of *concurrent processes*.

Some challenges were identified, namely the challenge to coordinate all activities and the communication between the different parties and persons involved. This challenge can be solved through the implementation of *concurrent processes* and, if needed, with support from specialised management processes and tools.

In order to enable the easy and effective implementation of the proposed model and remedy any challenges pertaining to it, the author proposes a prototype to be used to provide guidance and for the implementation of the proposed process model. The next part of the thesis presents the proposed prototype.

PART 4: PROTOTYPE

The first chapter of **Part 4** proposes a prototype to be used to provide guidance and for the implementation of the proposed process model. The proposed prototype has two main functional aims. The first aim is to provide guidance in implementing the proposed process model and the second aim is to enable the investigators to implement the model through use of convenient software application while reliable logging actions in order to be able to validate the use of the proposed process model.

The second chapter presents the results of the evaluation of the proposed prototype with regard to its software usability and in terms of whether the prototype meets the requirements.

CHAPTER 7- PROTOTYPE FOR GUIDANCE AND IMPLEMENTATION OF A COMPREHENSIVE AND HARMONISED DIGITAL FORENSIC INVESTIGATION PROCESS

7.1 Introduction

In this chapter the author proposes a prototype for guidance and implementation of a comprehensive and harmonised digital forensic investigation process. The chapter explains the proposed prototype, its potential use and benefits.

(Note that the author already published a paper on the proposed prototype [76].)

Please refer to **Appendix D** for the user guide for the proposed prototype in order to get full appreciation of its software functionality and usability. Refer to **Appendices E and F** for source code of the proposed prototype.

7.2 Prototype overview

The prototype is in the form of a software application that has two main functionalities. The first main functionality is to act as an expert system that can be used for guidance and training novice investigators. The second main functionality is to enable the implementation of the investigation process, while reliably logging all actions in a digital forensic fashion. Ultimately, the latter functionality should enable the validation of use of a proper digital forensic investigation process.

The use of the proposed software (prototype) would significantly help any organisation involved in digital forensic investigations to follow the process proposed in this thesis and enhance the admissibility of digital evidence and the results of investigations. Also, the software can be used by organisations involved in or providing training in the field.

Another goal in designing the prototype is to maximise and encourage collaboration between different organisations by allowing them to work together on a case from any location.

For illustration purposes only, **Figure 7.1** presents a screenshot of the Graphical User Interface showing the *readiness processes* class and, specifically, the *scenario definition*

process. It is intended to allow one to follow the processes as prescribed by the standardised process model [21].

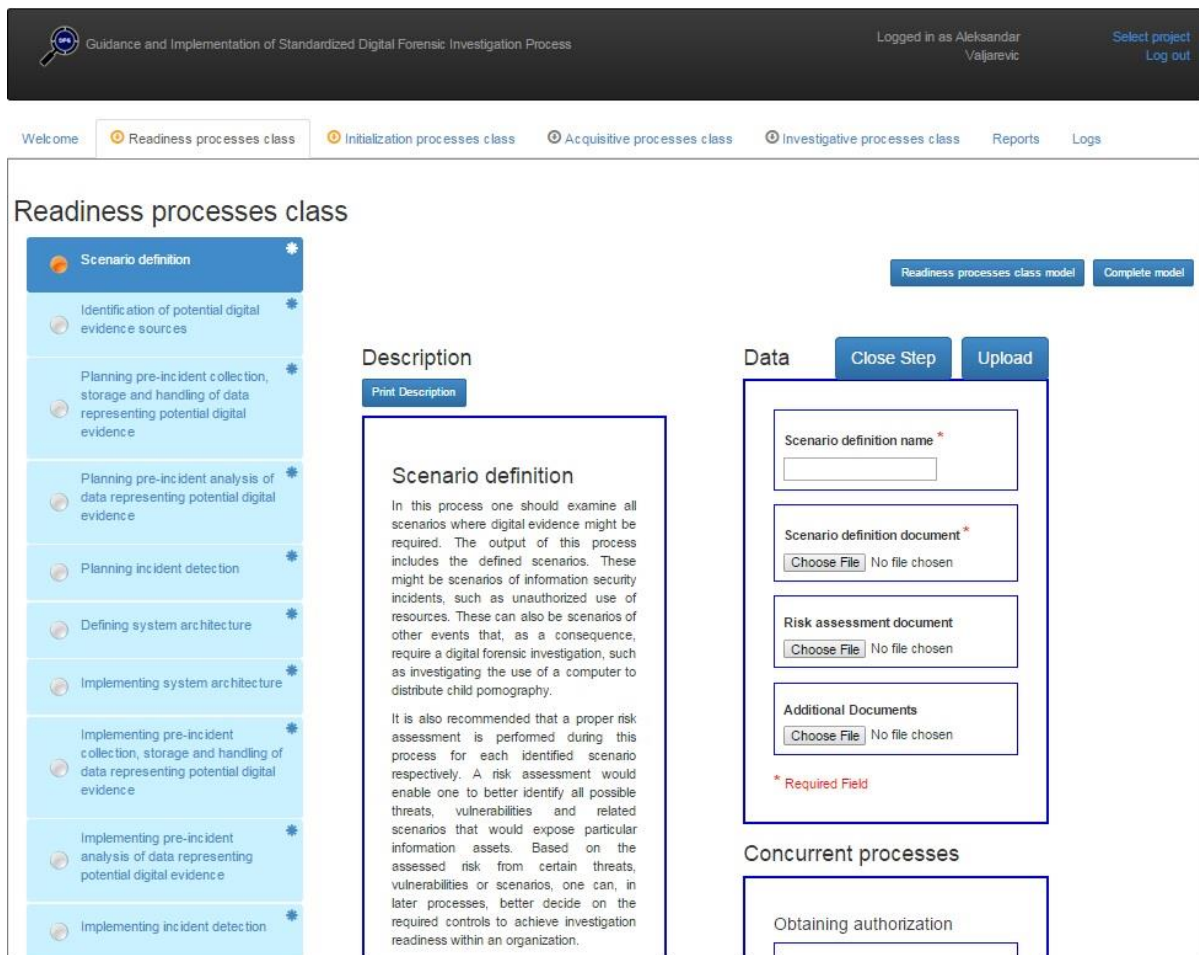


Figure 7.1 Prototype Graphical User Interface

The software provides guidance (on the left side of the user pane) and the possibility to implement the process (on the right side of the pane). The user can freely browse the guidance on any step; however he/she will only be able to implement the steps in accordance with the defined process sequence. The user can also choose to generate reports through selecting the *Reports* tab from the task bar at the top.

The information system security is based on the use of cryptographic technologies to ensure effective access control, confidentiality and integrity of all information.

Non-repudiation of user actions is enabled through the use of digital signatures. This also serves to verify the authenticity of actions and to verify any associated information (files) as

accessed by the user. The following section explains the system layout, which includes the following:

- Software development lifecycle
- System architecture
- Components
- Information system security

7.3 Software development lifecycle

This section gives an overview of the software development lifecycle used for the development of the prototype, namely Rapid Application Development (RAD) [82]. RAD has two main characteristics. It is a methodology that prescribes phases in software development. It is also a class of tools that allow fast object development, graphical user interfaces, and reuse of code.

RAD was chosen because of the nature of the prototype and the fact that the development required a fast-paced framework in which the ‘client’ is constantly involved. The development of this prototype also required a semi-flexible lifecycle as the representation of the models were likely to change during the development of the prototype.

RAD also catered for the time constraints and worked well with a single developer team because it promotes communication between the ‘client’ and the developer.

7.4 System architecture

This section gives an overview of the system architecture, and the focus is placed on technology components that were used to realise the prototype (software).

Database – The database was implemented using MySQL [83], which was chosen because it is free, fast and cross-platform. MySQL includes data security layers to protect data from intruders, passwords are encrypted and rights can be set up to allow access to specific users only.

Platform – The platform chosen for the prototype was web-based as this would allow ease of use across multiple platforms and from any location. It facilitated the collaboration of

multiple users from multiple organisations. It would also be better to provide the prototype as a Software as a Service (SaaS) [84] because the user then has no control over the server thus it can be optimised for complete security by the owner. SaaS also provides better cost effectiveness for the user and enables the user to concentrate on the core activity- the digital forensic investigation.

Language and framework – The prototype was implemented using the PHP [85] coding language and the Laravel Framework [86]. Laravel is a free, open source PHP web application framework, designed for the development of MVC (Model-View-Controller) web applications [87, 88]. The Laravel framework was chosen because of its MVC and REST (Representational State Transfer) capabilities, as well as its database support and available add-ons and libraries. Laravel also has a number of important security-related functionalities such as encryption and authentication.

User management – For user management, Sentry [89] was used. Sentry is an add-on to Laravel that provides configurable user management and it is interface driven. Sentry also encrypts all passwords and allows an easy way to authenticate a user and to prevent access to pages based on the user that is logged in.

Report generator – For generating reports, the tool: *wkhtmltopdf* [90] was used. *wkhtmltopdf* is an open source command-line tool to change HTML (HyperText Markup Language) into PDF (Portable Document Format) by using the QT Webkit rendering engine [91]. This tool does not require a display or display service. The NitMedia [92] wrapper was used to combine the tool easily within Laravel. This wrapper converts the normal *wkhtmltopdf* package into a composer package that is usable in the Laravel framework.

Component communication architecture – All components (see **Section 7.5**) communicate by using the Representational State Transfer (REST) architecture [93]. REST is an architectural style that consists of components, connectors and data elements for distributed web systems.

Section 7.5 concentrates on the functional components of the prototype.

7.5 Components

This section describes the functional components of the prototype and their interaction.

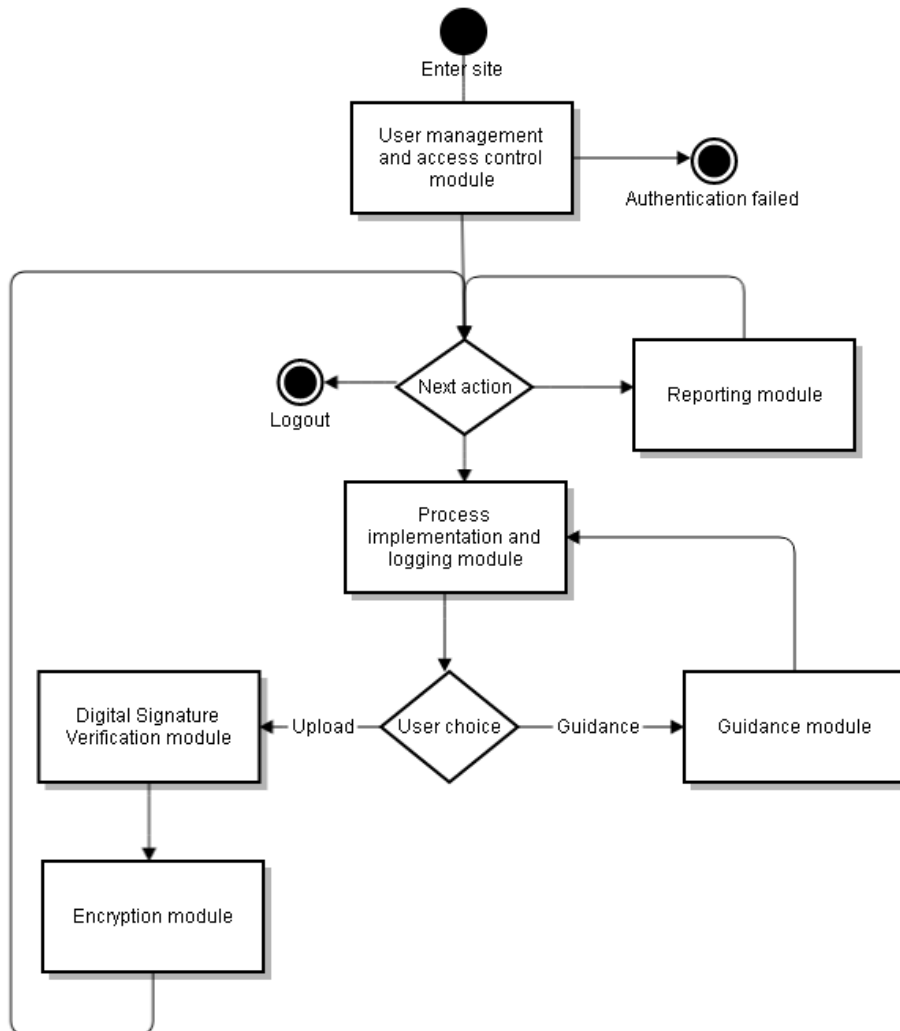


Figure 7.2 Basic interaction diagram

Figure 7.2 shows the high-level interaction between the modules.

When users enter the site, they will be passed through the user management and access control module where they will be authenticated and their permissions will be checked. If authentication fails, the users will be asked to log in again. If login succeeds, they will be able to choose whether they want to generate a report (passing them through the reporting module), logout or implement a step. If the users choose to implement a step, they will be able to choose whether they want to view the guidance (passing them through the guidance module) or upload data to a step (passing the data through the digital signature verification module as well as the encryption module).

User management and access control module – This module is responsible for managing user authentication and access control. Access control is role based; meaning only users with the correct roles are allowed to access certain projects (digital forensic investigations), data and functionalities of the software. All users are allowed to close or reopen a step (as explained in the *Process implementation and logging module* section). When reopening a step, the user will have to give a reason for doing that.

The software currently has the following predefined roles for the users:

- **Root** – In this role, the user has access to all functions.
- **System overseer** – This user has the required access to implement all steps.
- **System owner**- This user has access to implementing all steps, as well as access to the administrative part of the application.
- **System custodian** – This user has access to implementing all steps inside the *readiness processes* class.
- **System administrator** – This user has access to implementing all steps in the *readiness processes* class, which follow after the *implementing system architecture* step.
- **First responder** – This user has access to implementing all steps in the *initialisation processes* class, as well as all steps in the *acquisitive processes* class.
- **Investigator** – This user has access to implementing all steps in the *initialisation processes* class, all steps in the *acquisitive processes* class, as well as all steps in the *investigative processes* class.
- **Analyst** – This user also has access to implementing all steps in the *initialisation processes* class, all steps in the *acquisitive processes* class, as well as all steps in the *investigative process* class.

- **Legal system representative** – This user has access to generating reports only.
- **Accused** – This user also has access to generating reports only.

In **Table 7.1** a comparison is drawn between the different roles and their permissions. Every role has access to generating a report for the currently logged-in user and the current project.

Table 7.1 Comparison of user roles

Role/Module	Admin	Readiness	Initialisation	Acquisitive	Investigative
Root	N	Y	Y	Y	Y
System overseer	N	Y	Y	Y	Y
System owner	Y	Y	Y	Y	Y
System custodian	N	Y	N	N	N
System administrator	N	Y	N	N	N
First responder	N	N	Y	Y	N
Investigator	N	N	Y	Y	Y
Analyst	N	N	Y	Y	Y
Legal system representative	N	N	N	N	N
Accused	N	N	N	N	N

The users in the System Overseer and System Owner role can generate reports for all users within their organisation.

A user can have more than one role in the system and will have access to all of the steps that are allowed by the combined roles.

7.5.1 Reporting module

This module is responsible for generating reports on users' actions. The reporting module is of crucial importance as it enables verification that a proper standardised process was followed and all guidelines and requirements were adhered to. The module will enable the creation of reports by authorised users, per project, user, concurrent process and organisation. Three types of reports can be created: a compliance report, a project report and a user report.

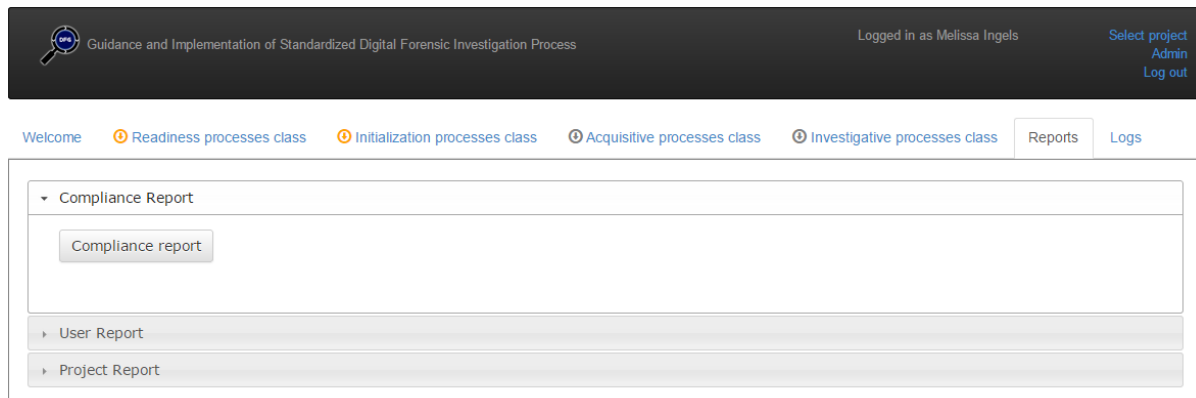


Figure 7.3 Details of the *reporting* module's Graphical User Interface

7.5.2 Process Implementation and Logging module

This module guides the user through the completion of the processes, as it allows him/her to choose a process and upload the documents for that process. From here the user can upload documents, enter data, view guidance, as well as generate reports. The user can also close or reopen a step. Closing a step prevents any further data from being uploaded to the step and enables the user to continue with the next step in the process. Reopening a step will reopen all steps that were implemented after the relevant step. When reopening a step, however, the user has to provide a reason for doing so. The reason can be used for audit purposes.

Scenario definition *

- Identification of potential digital evidence sources *
- Planning pre-incident collection, storage and handling of data representing potential digital evidence *
- Planning pre-incident analysis of data representing potential digital evidence *
- Planning incident detection *
- Defining system architecture *
- Implementing system architecture *
- Implementing pre-incident collection, storage and handling of data representing potential digital evidence *
- Implementing pre-incident analysis of data representing potential digital evidence *
- Implementing incident detection *
- Assessment of implementation *
- Implementation of assessment results *

Data Close Step Upload

Scenario definition name *

Scenario definition document *

Risk assessment document

Additional Documents

* Required Field

Concurrent processes

Obtaining authorization

Documentation

Managing information flow

Name

Encryption/security measures used

Information flow document

* Required Field

Close Step Upload

Figure 7.4 Details of the *process implementation and logging* module's Graphical User Interface

7.5.3 Guidance module

This module provides guidance to the user in terms of how the process should be implemented – through providing either graphical or textual advice, or both. This component is optional to the user. The guidance module is especially intended for use by novice investigators or other novice professionals involved with digital forensic investigations.

Description

[Print Description](#)

Scenario definition

In this process one should examine all scenarios where digital evidence might be required. The output of this process includes the defined scenarios. These might be scenarios of information security incidents, such as unauthorized use of resources. These can also be scenarios of other events that, as a consequence, require a digital forensic investigation, such as investigating the use of a computer to distribute child pornography.

It is also recommended that a proper risk assessment is performed during this process for each identified scenario respectively. A risk assessment would enable one to better identify all possible threats, vulnerabilities and related scenarios that would expose particular information assets. Based on the assessed risk from certain threats, vulnerabilities or scenarios, one can, in later processes, better decide on the required controls to achieve investigation readiness within an organization.

This will enable an organization to take into account the risk level, costs, and benefits of possible controls in a bid to reduce the identified risk

Figure 7.5 Details of the *guidance* module's Graphical User Interface - textual advice

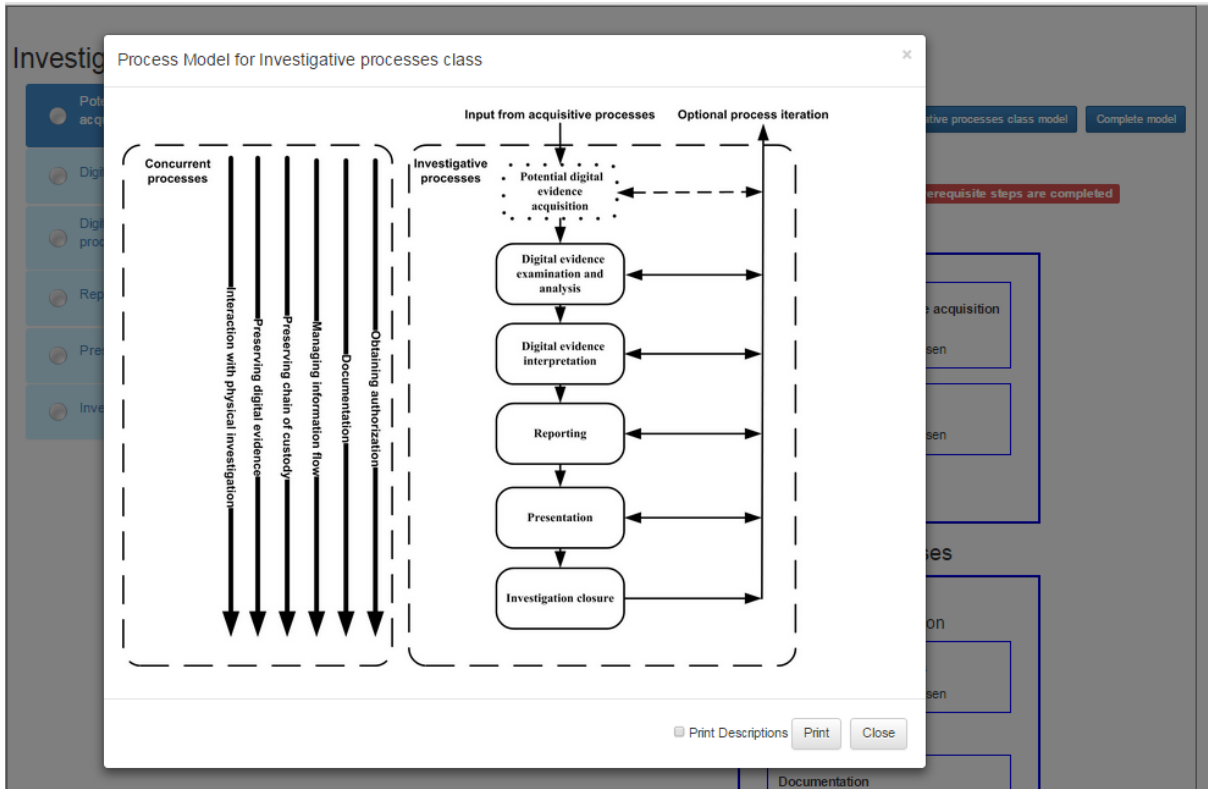


Figure 7.6 Details of the *guidance* module's Graphical User Interface - graphical advice

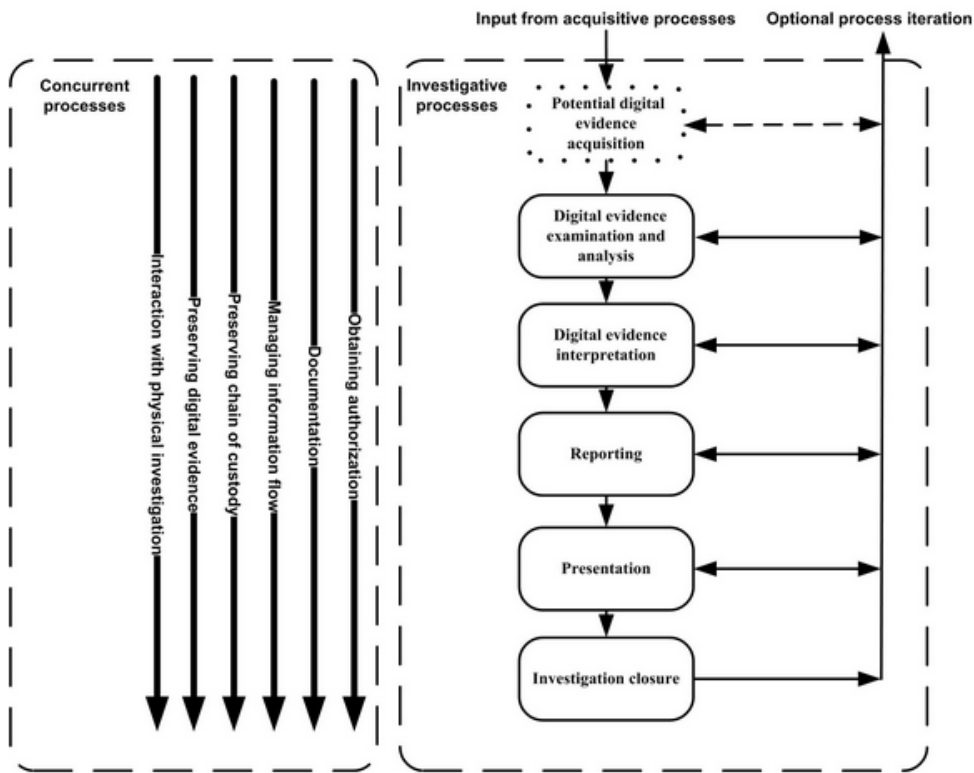


Figure 7.7 Details of the *guidance* module’s Graphical User Interface - graphical advice zoomed in

7.5.4 Digital signature verification module

When the user uploads a document, this module will verify that the document was digitally signed by the user who attempted to upload it. The user will have to digitally sign the document (using the certificate generated by the user management and access control module) prior to uploading it into the system. The prototype requires the user to digitally sign the document so as to preserve the integrity of documents as promoted by the standard. If a document is not signed by the right user, the system will reject it and ask the user to upload a signed document. For prototype purposes, verification is only done on .pdf, .docx (MSWord 2010) and .xml (EXtensible Markup Language) files.

7.5.5 Encryption module

The encryption module is responsible for the encryption of all textual data entered by the user, as well as any files uploaded by the user. The data is encrypted in such a manner that only authorised users can access it. This module uses AES256 [94] to encrypt the textual data and files. The key for the encryption is stored on the server so that risk of compromising the key on user side is minimised.

The next section explains the sequence of action within the prototype (software) and interactions between the components in more detail.

7.6 Activity diagram for the main application

Figure 7.8 presents a prototype component activity diagram. This diagram, which is an extension of **Figure 7.2**, shows the interaction between the components and sequence of actions within the prototype. The numbers appearing in **Figure 7.8** relate to the numbers in brackets in the explanation of the activity diagram that follows below.

The activity within the prototype software starts with the user accessing the website (1) of the prototype. If the user is not logged in, he/she is redirected to the login page (2), where he/she can log in and the system will authenticate his/her credentials (3). If the user is logged in, his/her roles will be checked to see if he/she has permission to access the page he/she is trying to access (4). If he/she does not have permission, he/she will get an error message (5) and will have to retry. If he/she does have the necessary permission, the start page will be loaded.

The user can then choose whether he/she wants to follow a process, make a report or log out (6).

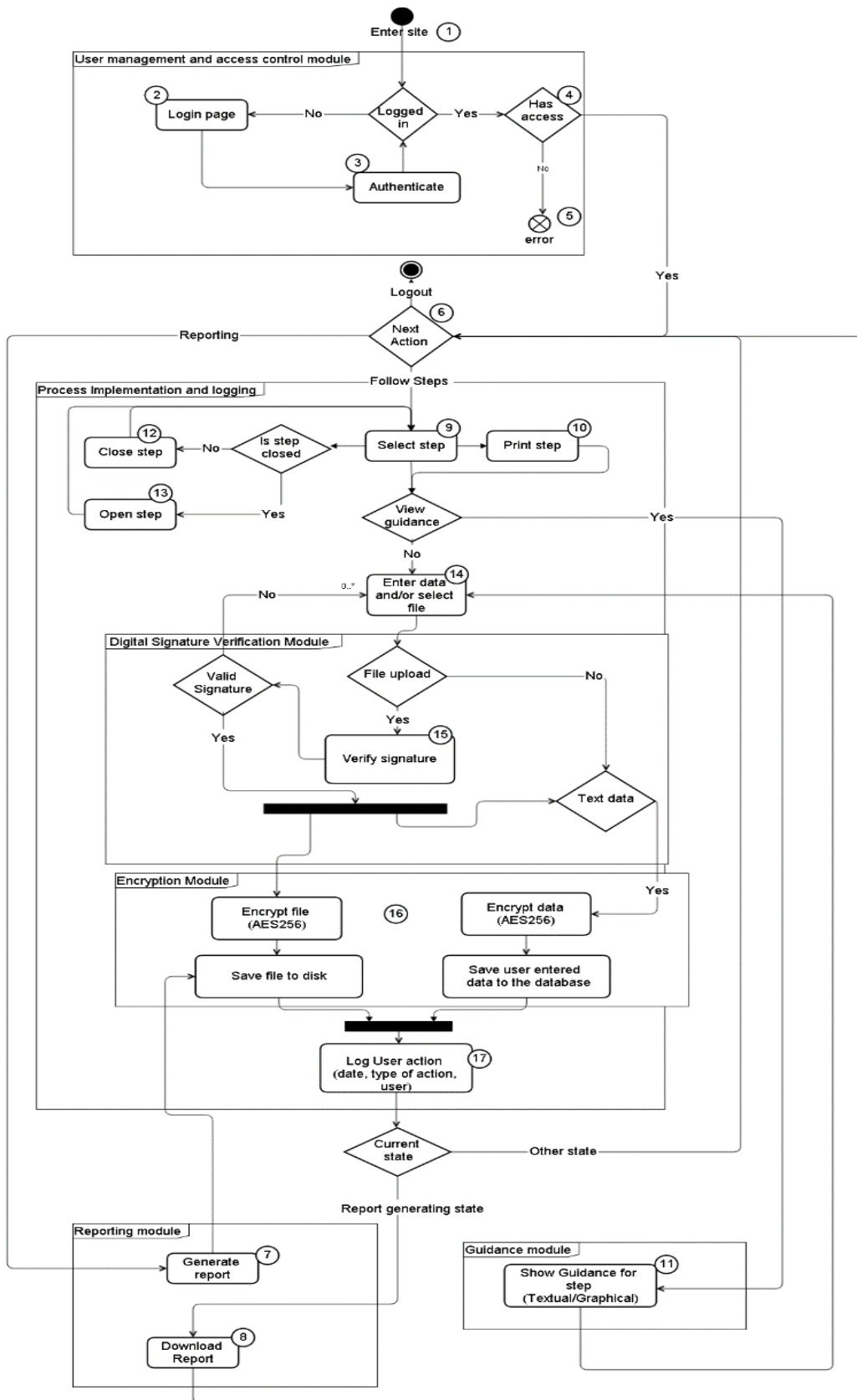


Figure 7.8 Activity diagram

If the user chooses to make a report, he/she will be shown the reporting page (7). The user will then be able to choose the report he/she wants to generate by clicking on the appropriate button. Report options will be limited to the roles of the logged-in user as explained in the *User management and access control module* section. The system will generate the report and save it to the disk, after which the user will be able to download the generated report (8). After either of these steps, the user will be able to choose whether he/she again wants to follow a process, make a report or log out from the prototype (6). If the user chooses to follow a process, he/she will be able to select the process he/she wants to view (9). The user will next be able to choose whether he/she wants to print the process (10), see guidance for the process (11), continue with the execution of the process, or close or reopen the step.

Printing the process would enable printing the guidance provided for the relevant step or guidance for the entire model.

If the user chooses guidance, he/she will see image and text data to guide him/her in executing the process. After that, he/she will be able to proceed with the process.

If the user chooses to close or open a step, he/she will be allowed to close (12) the step (if the step is not yet closed) or open (13) the step (if the step is already closed). Both actions will allow the user to choose a new step to implement.

When executing the process, the user can input the data requested by the process and upload any necessary files (14). The system will verify the digital signatures (15) if a file was uploaded and then encrypt both the user data entered into predefined forms and the files that were uploaded (16). The encrypted and signed files will be saved to the disk. The encrypted data entered by the user will be saved to a database. The user can verify that the data was uploaded into the system by viewing the logs for the relevant step at the bottom of the page.

The process name, date, user name, description of all activities and any other relevant information will be logged to the database for audit purposes (17).

Once a process is closed, the user will be able to again choose whether he/she wants to follow a new process, make a report or logout (6).

If the user logs out, he/she will be redirected to the logon page and the process will start over.

7.7 Functionality of the admin module of the prototype

The admin module is accessible only to the System Owner. The data displayed in the respective admin pages is also limited to the access that the user has. The Root admin role has access to the admin section with no restrictions in terms of what the user can view, edit, add or delete. This role is intended for the prototype owners that manage the entire system. The reason for the restriction placed on the System Owner's role is to protect the confidentiality of the users and the integrity of the system.

Next follows the explanation of the different sections inside the Admin section. The explanations are written with the restrictions of the System Owner role.

Please refer to **Figures 7.9, 7.10 and 7.11** for Graphical User Interface of the admin module.

7.7.1 User section

The User section allows the currently logged-in user to view and edit the users who are part of his/her organisation. This section also allows the logged-in user to generate a digital certificate for the users he/she is allowed to view. When the user generates a digital certificate, the system will pull information from the organisation in which the chosen user is and generate a digital certificate with a password. The number of certificates generated for a user is logged to the database. The currently logged-in user can then decide how to provide the information to the user. The currently logged-in user can also add a new user to the system. This newly added user will automatically be added to the organisation that the currently logged-in user belongs to. When adding or editing a user, the currently logged-in user can select the roles that will be assigned to such user. Deleting the user will ban the user account and prevent the user from logging into the system. The delete process can be undone, thus allowing the user to log in again. A user is never completely deleted from the system due to reports, logs and other data that are connected to the user.

Webpage Screenshot

DFG Admin

- [Home](#)
- [Organisations](#)
- [Users](#)
- [Projects](#)
- [Return to site](#)

Users

Show deleted users

Email	First name	Last name	Roles	Created at	Updated at	Certificates generated	Operations
peppercat101@gmail.com	Melissa	Ingels	System overseer Prototype Owner	2015-01-30 21:28:02	2015-02-02 18:09:08	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Generate certificate"/>
aleksandar.vajjarevic@gmail.com	Aleksandar	Vajjarevic	System overseer	2015-01-30 21:28:02	2015-01-30 21:28:02	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
System_owner@gmail.com	System owner	_T	System owner	2015-01-30 21:28:02	2015-01-30 21:28:02	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
System_custodian@gmail.com	System custodian	_T	System custodian	2015-01-30 21:28:02	2015-01-30 21:28:02	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
System_administrator@gmail.com	System administrator	_T	System administrator	2015-01-30 21:28:03	2015-01-30 21:28:03	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
First_responder@gmail.com	First responder	_T	First responder	2015-01-30 21:28:03	2015-01-30 21:28:03	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
Investigator@gmail.com	Investigator	_T	Investigator	2015-01-30 21:28:03	2015-01-30 21:28:03	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
Analyst@gmail.com	Analyst	_T	Analyst	2015-01-30 21:28:03	2015-01-30 21:28:03	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation
Legal_system_representative@gmail.com	Legal system representative	_T	Legal system representative	2015-01-30 21:28:03	2015-01-30 21:28:03	0	<input type="button" value="Edit"/> <input type="button" value="Delete"/> User is not in an organisation

http://localhost/prototype/public/admin/users Mon Feb 02 2015 20:09:23 GMT+0200 (South Africa Standard Time)

Figure 7.9 Details of the *admin* module’s Graphical User Interface - user section

7.7.2 Organisation section

This section allows the currently logged-in user to view the organisation of which he/she is a part. It also allows the user to add or remove users from his/her organisation. Removing a user from an organisation will disable the user account, which means the user will no longer be able to log in. Adding a user to an organisation will (re-)enable his/her account. Only users who are not part of an organisation can be added to the organisation. When editing the organisation, the user will be able to change the name as well as choose which other organisations are allowed to see his/her organisation's users. This is to promote collaboration between different organisations and to allow one organisation to add another organisation's users to its projects.

7.7.3 Project section

This section allows the currently logged-in user to add, edit or close/reopen a project. It also allows the user to add or remove users from the project. When adding users to a project, the currently logged-in user will be able to see all the users in his/her organisation, as well as users from organisations that have given permission to the currently logged-in user's organisation to see their users. When the user closes a project, it disables the project from being worked on. However, the project can be accessed from the Reports section in order to generate reports in the future. A project can be reopened if it has been closed to enable the implementation of additional steps.

Webpage Screenshot

DFG Admin

- Home
- Organisations
- Users
- Projects
- Return to site

Organisations

[Add](#)

Name	Organisations allowed to see use	Created by	Organisations allowed to see use	Created at	Modified at	Operations
The owners organisation	The owners organisation	Melissa Ingels		2015-01-30 21:28:03	2015-01-30 21:28:03	Edit Add Users Delete

Users

Email	First name	Last name	Last login	Operations
aleksandar.valjarevic@gmail.com	Aleksandar	Valjarevic		Remove
Prototype_Owner@gmail.com	Prototype Owner	_T		Remove
peppercat101@gmail.com	Melissa	Ingels	2015-02-02 18:09:08	Remove

Figure 7.10 Details of the *admin* module’s Graphical User Interface - organisation section



Webpage Screenshot

DFG Admin

- Home
- Organisations
- Users
- Projects
- Return to site

Projects

[Add](#)

Name	Case number	Created by	Created at	Modified at	Open	Operations
Incomplete Example Project	Case #257	Melissa Ingels	2015-01-30 21:32:45	2015-01-30 21:32:45		Edit Add Users Delete
Completed Example Project	Case #456	Melissa Ingels	2015-01-30 21:32:45	2015-01-30 21:32:45		Edit Add Users Delete

Users

Email	First name	Last name	Last login	Operations
peppercat101@gmail.com	Melissa	Ingels	2015-02-02 18:09:08	Remove

Figure 7.11 Details of the *admin* module's Graphical User Interface - project section

The next section is dedicated to the implementation of information system security.

7.8 Information system security

This section explains the basics of the information systems security of the prototype.

The system implements the encryption of user files and data by using the AES256 (Advanced Encryption Standard 256) [94] algorithm. It also implements verification of digital signatures to ensure the integrity and confidentiality of all data.

All connections to the server are encrypted through an HTTPS using either SSL 3 (Secure Socket Layer 3) or any version of TLS (Transport Layer Security) protocols – based on what the user’s browser supports. If the browser does not support either of these two protocols, the user will be asked to first upgrade his browser.

7.9 Discussion on the proposed prototype

The proposed prototype enables one to easily follow the proposed process model, and this eventually results in the higher admissibility of digital evidence and findings of digital forensic investigations. Higher admissibility of digital evidence and other results of digital forensic investigations would be possible due to the fact that courts of law would probably be more satisfied that a standardised and formalised process, which had passed significant peer review and was ultimately accepted as an international standard [21], was followed during a digital forensic investigation.

Another use of such a prototype is the fact that it would provide for the training of novice investigators. The possible improvement in efficiency and effectiveness of digital forensic investigations would prove to be a further benefit, due to the fact that clear process guidelines are available.

The two main functionalities that provide the benefits as explained above are acting as an expert system that can be used for guidance and training of novice investigators, and enabling the implementation of the investigation process while reliably logging all actions in a digital forensic fashion.

The author proposed a well-defined architecture for the prototype and defined key functional components, while taking into consideration information systems security. A web-based platform was chosen to develop the prototype in order to cater for multiple users from multiple locations and jurisdictions, with minimal requirements for client infrastructure. Cryptography was used to ensure the integrity of all information, as well as to ensure non-repudiation of user actions.

The author believes that the proposed prototype constitutes a significant step towards facilitating the implementation of a standardised digital forensic investigation process model. The proposed prototype not only enables implementation, but also the logging and non-repudiation of all user activities, with special focus on *concurrent processes* that cater for evidence integrity.

The next section concludes the chapter.

7.10 Conclusion

In **Chapter 7** the author presented the proposed prototype and gave an overview of functionalities, architecture and components. After this, the benefits of use of such a prototype were discussed.

(As was mentioned earlier, please refer to **Appendix D** for the user guide for the proposed prototype in order to get a full appreciation of the software functionality and usability. Also refer to **Appendices E and F** for source code of the proposed prototype.)

The proposed prototype was evaluated for usability and effectiveness. **Chapter 8** of this thesis presents the results of testing the proposed process prototype in a real-world context.

CHAPTER 8- EVALUATION OF THE PROPOSED PROTOTYPE

8.1 Introduction

In this chapter the author presents the results of analysis of the implementation of the proposed. A usability test and survey were designed and performed to evaluate the usability of the system. Another survey, referred to as the Functional survey, was set up to evaluate whether the prototype meets the goals proposed in this thesis. The latter survey was also included questions aimed at improving the prototype.

The usability testing survey was based on the Software Usability Measurement Inventory (SUMI) measurement method provided by SUMI [95]. The Software Usability Measurement Inventory is a rigorously tested and proven method of measuring software quality from the end user's point of view [95]. It consists of 50 statements to which the user has to reply that they either 'Agree', 'Don't Know', or 'Disagree' [95]. Answers are then used to evaluate software's quality as per method developed by SUMI [95].

The Functional survey was set up by the author and fellow students from ICSA research group at University of Pretoria.

The testing process was designed as an assignment for students taking the Digital Forensics course at the University of Pretoria. All students were final-year students busy completing their BSc in Computer Science. The students were requested to apply the proposed process model, with provided scenarios, and use the prototype as guidance. A total of 32 students participated in the testing, which is more than 20 as recommended by SUMI [95] as a minimum number of participants.

Next follows a basic overview of the results gained from both surveys.

8.2 Usability testing results

The report of the usability testing survey was provided by the SUMI organisation and the results were divided into a global scale and the following five subscales:

- Efficiency – How well can the user achieve his/her goals using the product?
- Affect – How well did the product capture the user’s emotional responses?
- Helpfulness – How well does the product assist the user?
- Control – How well does the user feel he/she is in control?
- Learnability – How easy is it for the user to learn to use the product?

SUMI uses a z-score transformation to make the scales have an expected mean of 50 with a standard deviation of 10. The prototype scored a global score of 43.62, which is within the general expected score, but the results indicate that the user interface should be improved.

Table 8.1 shows the mean, standard deviation, median, interquartile range (IQR), minimum and maximum scores in each subscale, as well as the global scale. As we can see from this table, Learnability got the highest score, which indicates that the prototype is relatively easy to learn and understand. Affect got the lowest score, which indicates that the prototype may have frustrated the users.

Table 8.1 Summary of SUMI results

	Mean	Standard Deviation	Median	IQR	Minimum	Maximum
Global	43.62	12.87	41	16	19	72
Efficiency	42.17	13.06	41	21	21	72
Affect	41.93	16.94	41	28	15	72
Helpfulness	46.55	13.34	44	18	21	72
Control	43.76	12.52	42	14	19	68
Learnability	49.93	14.50	55	22	19	71

The other subcategories scored a mean of between 42 and 46, which indicated that they could also be slightly improved but was overall good.

We can see from the Minimum and Maximum values that some users were very satisfied while others were not. The highest scores are usually at around 72, while the lowest scores are usually around 19. The interquartile range (IQR) values are given as a reference.

Figure 8.1 presents a graphical view of the means and standard deviations under each subscale.

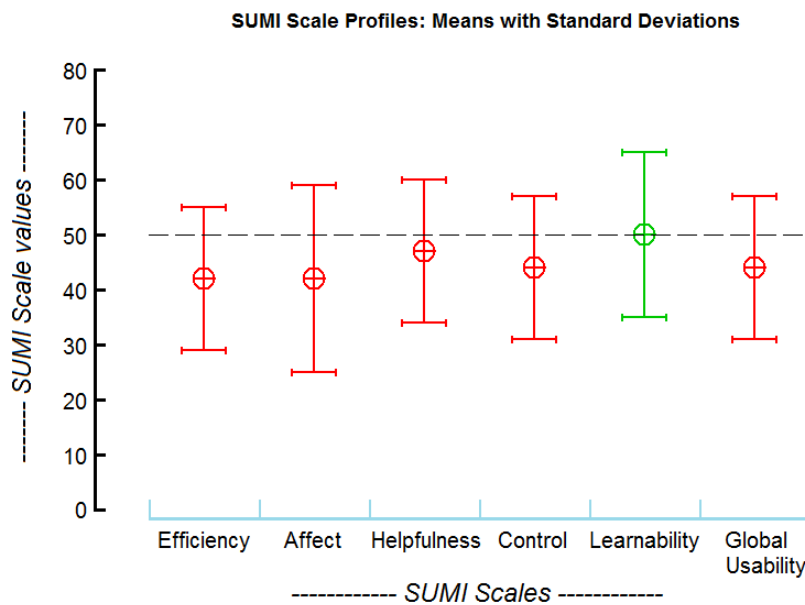


Figure 8.1 SUMI scale profile of the proposed prototype

We analysed the user answers with regard to what they considered to be the best aspect of the prototype. Most users indicated that the logical outline of the software and the step-by-step guide constituted the best aspect. Others indicated that the design, guidance and response time were the best aspect for them.

We also analysed the responses with regard to what users thought should be improved. The majority of users indicated that the error messages provided should be more elaborate and that the guidance and help could be improved. Other users also indicated that there were a couple of minor bugs that need attention.

8.3 *Functional survey results*

During the analysis of the functional survey the authors have requested participants to rate the prototype in regards to reaching the prototype goals. Participants were asked to rate the whether the following goals have been reached:

- Guidance for the model
- Understanding of the model
- Usefulness
- Collaboration
- Accessibility
- Manual usefulness
- Guidance usefulness
- Flow of the system

The authors calculated the average score (out of 5) for each section. The results are indicated in **Table 8.2**.

Table 8.2 Summary of the functional survey results

Section	Average rating
Overall system rating	3
Guidance for the model	4
Understanding of the model	4
Usefulness	4
Collaboration	3
Accessibility	4
Manual usefulness	3
Guidance usefulness	3
Flow of the system	3

The results indicate that the usefulness of the guidance provided by the manual and usefulness of the flow and collaboration in respect of the prototype could be improved. The analysis also indicated that 87% of the users used the provided guidance and 50% of the users used the manual along with the software.

Analysis of the various comments indicated that error messages should be clearer and that there are still a number of minor bugs, especially concerning the signature checking on files. Results also indicated that guidance can be improved. The users indicated that they thought that the system could be very useful and that it helped them to understand the flow of the proposed model. Various users also suggested that the software should tie in with existing forensic investigation tools.

In terms of reports, the results showed that 90% of the users understood the reports and the main suggestion was to add more descriptions.

8.4 Discussion on the evaluation of the prototype

The prototype enables one to easily follow the proposed process, and this should result in higher admissibility of the digital evidence and results obtained in digital forensic investigations. Such evidence and findings of digital forensic investigations would also be accepted to a much larger extent, since courts of law are likely to be more satisfied that a standardised and formalised process was followed during a digital forensic investigation.

The usability testing and evaluation confirmed the overall good quality of the prototype and verified that it indeed complied with the necessary functional requirements. A logical outline and step-by-step guidelines were identified as the most positive factors, while the testing and evaluation also showed that there was a need for improvement of the user interface, especially in respect of error messages and help.

Based on the usability and effectiveness test performed and after analysing the current state of the proposed prototype, the author identified potential areas of future work pertaining to prototype software development. The author plans to extend this prototype by improving its usability, allowing users to upload predefined XML files with keywords and compile large sets of data into documents so that the user does not have to. Other improvements that can be made to the prototype include signing the digital certificates of users with a CA (Certificate Authority) issued root certificate. The author furthermore plans to introduce the ability to revoke certificates and manage a complete Public Key Infrastructure. Ultimately the author and his fellow researchers want to implement a system where the user does not have to digitally sign a document before uploading it. They rather plan to change the system to add functionality to its back-end to automatically digitally sign a document by using the relevant user certificate when the document gets uploaded. The author also intends to implement the proposed changes and improvements gathered from the evaluation testing. After implementation, the author plans to run these tests again to evaluate how well the changes were implemented.

The next section concludes the chapter.

8.5 *Conclusion*

In this chapter the author presented evaluation of the proposed prototype.

It can be concluded that the prototype should be useful to investigators who perform digital forensic investigations, especially since it ensures that a formalised and standardised process is followed.

We can also conclude that the system is relatively easy to learn. It does however require some future work, especially in respect of user interface, error messages and help.

The prototype is a significant step towards enabling the implementation of a standardised digital forensic investigation process model. The prototype enables not only implementation but also logging and non-repudiation of all user activities, with a special focus on concurrent processes, which cater for evidence integrity. This should ultimately add to the higher admissibility of evidence in court of law.

PART 5: ISO/IEC 27043:2015 INTERNATIONAL STANDARD

This part consists of one chapter. **Part 5** presents the international standard on a digital forensic investigation process and related standards, which is the result of the author's engagement with ISO and the model proposed in this thesis. In **Part 5**, the author also compares ISO/IEC 27043:2015 [21] and related standards to explain the role, uniqueness and comprehensiveness of ISO/IEC 27043:2015 [21].

CHAPTER 9- ISO/IEC 27043:2015 INTERNATIONAL STANDARD

9.1 Introduction

The result of the author's engagement with ISO is a new international standard ISO/IEC 27043:2015 [21]. The model proposed in this thesis represents the basis of this standard.

In this chapter the author gives an overview of both the standard itself and of related standards so as to enable the reader to understand the ecosystem of standards relating to the digital forensic investigation process. Furthermore, the author compares the ISO/IEC 27043:2015 [21] and related standards to explain the role, comprehensiveness and uniqueness of ISO/IEC 27043:2015 [21].

9.2 About this international standard

The ISO/IEC 27043:2015 international standard, titled "Information technology — Security techniques — Investigation principles and processes" [21] was published in March 2015. It defines an idealised model for the digital forensic investigation process. The model is intended to be used for various types of digital forensics, from post-mortem to cloud forensics and also in various investigation scenarios, including (but not limited to) criminal and civil cyber-crime cases, and corporate digital forensic investigations. Security incidents that are investigated can be criminal in nature or not. They can also range from serious cyber-attacks to critical infrastructure information systems (such as ports and power supply networks) to investigations into the unauthorised use of a company's IT resources for personal matters (such as use of the company's internet to access social media).

The basis of the standard is a comprehensive and harmonised digital forensic process model as presented in this thesis. The standard is the crown of the author's work and efforts towards achieving standardisation in the field by proposing a comprehensive and harmonised process model to be followed when performing digital forensic investigations.

The motivation for this standard has been to provide clear high-level guidelines for digital forensic investigation processes. The following additional needs were identified and considered [21]:

1. A need for establishing guidelines for investigation principles and processes that would expedite digital forensic investigations;
2. A need for guidelines that would allow for proper training of inexperienced investigators;
3. A need for guidelines that would assure flexibility within an investigation due to the fact that many different types of digital investigations are possible;
4. A need for establishing a harmonised digital forensic process model for criminal and civil prosecution settings, as well as in other environments;
5. A need for providing succinct guidance on the exact process to be followed during any kind of digital investigation in such a way that, if challenged, no doubt should exist as to the adequacy of the investigation process followed during such an investigation.

This international standard is intended to complement other standards and documents that provide guidance on the preparation for and actual investigation of information security incidents.

The standard, being the same as the process model proposed in this thesis, is not a detailed, low-level guide, but rather a guide that provides a wide overview of the entire incident investigation process [21]. In other words, the standard covers the width of the investigation process, but not its depth. The standard also establishes fundamental principles that are intended to ensure that tools, techniques and methods can be selected appropriately and be shown to be fit for the purpose, should the need arise [21]. Last but not least, the standard intends to help determining the reliability of digital evidence gathered as a result of the digital forensic investigation process.

It is envisaged that the standard will be used by organisations that need to protect, analyse and present potential digital evidence, and basically by any organisation that will be involved in digital forensic activities at any level and at any stage of the process [21].

This standard is furthermore relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence [21].

Therefore it should be applied by national and international bodies such as international and national law enforcement and justice agencies, national standardisation bodies, working groups relating to the digital forensics field, etc. It should also be used by private institutions when developing procedures, tools, methods and techniques in the area of digital forensic investigations. For example, the standard should be used by private digital forensic investigation laboratories as well as by any organisation that aims to achieve digital forensic readiness or that wishes to build capacity to be able to internally perform digital forensic investigations.

9.3 Related standards

The ISO/IEC 27043:2015 international standard [21], as explained above, is a high-level overarching guideline that covers the full width of digital forensic investigation processes.

We can call it an “umbrella standard” for digital forensic investigations. It provides guidelines for the complete course of a digital forensic investigation (including digital forensic readiness activities) and establishes a basis for performing digital forensic investigations in a uniform manner (from a processes and principles perspective). It can be applied across different types of digital forensic investigation and across borders and jurisdictions.

The ISO/IEC 27043:2015 is an international standard that is intended to complement other standards and documents that give guidance on preparations for and the actual investigation of information security incidents [21].

This international standard describes part of a comprehensive investigative process that includes, but is not limited to, the following topic areas [21]:

- Incident management, including preparation and planning for investigations
- Handling of digital evidence
- Use of and issues caused by redaction
- Intrusion prevention and detection systems, including the information that can be obtained from these systems

- Security of storage, including sanitisation of storage
- Ensuring that investigative methods are fit for the purpose
- Analysis and interpretation of digital evidence
- Understanding the principles and processes of digital evidence investigations
- Security incident event management, including the derivation of evidence from systems involved in security incident event management
- Relationship between electronic discovery and other investigative methods, as well as the use of electronic discovery techniques in other investigations
- Governance of investigations, including forensic investigations

Other international standards also address the above mentioned topics, but on a different level. Moreover, no other international standard encompasses all the activities and processes that are part of a digital forensic investigation in such a comprehensive manner.

The above topic areas are addressed, in part, by the following ISO/IEC standards [21]:

- **ISO/IEC 27037 [96]**

This international standard describes the means by which those involved in the early stages of an investigation, including initial response, can assure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

- **ISO/IEC 27038 [97]**

The digital redaction of documents is a relatively new area of document management practice, and it raises unique issues and potential risks. Where digital documents are redacted, removed information must not be recoverable. Hence, care needs to be taken that redacted information is removed permanently from the digital document (i.e. it must not simply be hidden within non-displayable portions of the document).

ISO/IEC 27038 specifies methods for the digital redaction of digital documents, as well as the requirements for software that can be used for redaction.

- **ISO/IEC 27040 [98]**

This international standard provides detailed technical guidance on how organisations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security involves the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and the security relevant to end-users during the lifetime of devices and media, as well as after end of use.

Security mechanisms like encryption and sanitisation can affect one's ability to investigate by introducing obfuscation mechanisms. These mechanisms have to be considered prior to and during the conduct of an investigation. They can also be important to ensure that storage of evidential material during and after an investigation is adequately prepared and secured.

- **ISO/IEC 27041 [99]**

It is important that methods and processes deployed during an investigation can be shown to be appropriate. This standard provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

- **ISO/IEC 27042 [100]**

This international standard describes how methods and processes to be used during an investigation can be designed and implemented to allow for the correct evaluation of potential digital evidence, interpretation of digital evidence, and effective reporting of findings.

The following ISO/IEC projects also address, in part, the topic areas identified above and can lead to the publication of relevant standards at some time after the publication of this international standard.

- **ISO/IEC 27035 (all parts) [101, 102, 103]**

This is a three-part standard that provides organisations with a structured and planned approach to the management of security incident management. It is composed of three parts:

- ISO/IEC 27035-1 [101]
- ISO/IEC 27035-2 [102]
- ISO/IEC 27035-3 [103]

- **ISO/IEC 27044 [104]**

This international standard provides guidance on the selection, implementation, use and management of Security Information and Event Management.

- **ISO/IEC 27050 (all parts) [105]**

This international standard provides guidance on the field of Electronic Discovery. It is concerned with the identification, preservation, collection, processing, review and production of digital evidence.

- **ISO/IEC 30121 [106]**

This international standard provides a framework for governing bodies of organisations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organisation for digital investigations before they occur. This standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access and cost effectiveness of digital evidence disclosure and it is applicable to all types and sizes of organisation. The ISO/IEC 30121 [106] is about the prudent strategic preparation of an organisation for digital investigation. Forensic readiness assures that an organisation has made the appropriate and relevant strategic preparations for accepting potential events of an evidential nature. Actions may occur as the result of inevitable security breaches, fraud and reputation assertion. In every situation, information technology (IT) has to be strategically deployed to maximise the effectiveness of evidential availability, accessibility and cost efficiency.

Figure 9.1 [21] shows typical activities that surround an incident and its investigation. The numbers shown in this diagram (e.g. 27037 [96]) refer to the international standards listed

above and the shaded bars show where each is most likely to be directly applicable or has some influence over the investigative process (e.g. by setting policy or creating constraints).

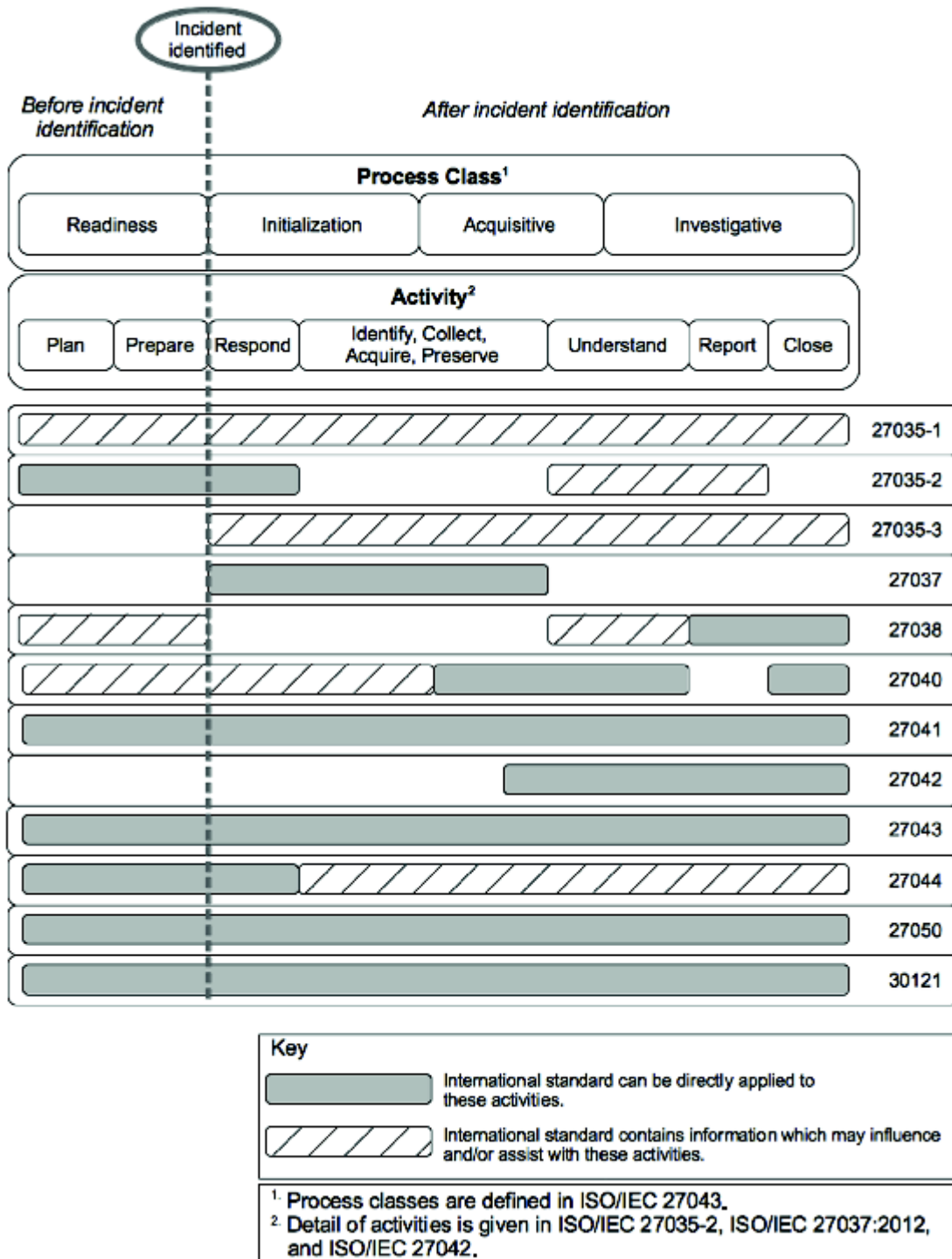


Figure 9.1 Applicability of standards to investigation process classes and activities [21]

9.4 Comparison of ISO/IEC 27043:2015 international standard with related standards

In order to emphasise the uniqueness and comprehensiveness of ISO/IEC 27043:2015 [21] when compared to other related international standards [96-106], the author will compare these based on the following qualitative characteristics:

- Area of concentration
- Area of application
- Level of detail
- Technology oriented or process oriented?

Please note that a similar comparison was performed when the model proposed in the thesis was compared to the existing digital forensic investigation process models. Although comparisons are based on similar characteristics, these two comparisons should not be confused. In the earlier comparison, we concentrated on the model proposed in the thesis and compared it to other models used for benchmarking. Now we are comparing the resulting ISO standard to related standards that do not include digital forensic investigation process models, but that concentrate on other aspects or more narrow fields of digital forensic investigation.

The author next gives an explanation of each of the characteristics listed above.

- Area of concentration

This characteristic defines the main area of concentration for the specific standard. Area of concentration describes subjects that the specific standard is concentrated on. The area can be a specific process or group of processes (for example incident response or analysis and interpretation), but it can also be a complete subject area (for example Electronic Discovery or Security Information and Event Management).

- Level of detail

This characteristic defines the level of detail that is present in specific standard. Standards can be high-level, if they provide high-level guidance and frameworks or when principles are presented. On the other hand standards can be of lower level, if they provide detailed and specific guidelines, processes, tools, methods or techniques.

- Area of application

This characteristic defines the intended, prescribed or envisaged application area of the specific standard. For example, the standard might be intended for use in any kind of digital forensic investigation or it can be intended for use in more specific applications such as Information and Event Management.

- Technology oriented or process oriented?

This characteristic defines if the specific standard is oriented towards processes or towards technology. Usually, high-level standards such as ISO 27042 [100] will be process oriented, while low-level standards will be technology oriented and will provide more technology-related details. Process-oriented standards are often technology neutral and do not favour or prescribe specific technologies or technological solutions. On the other hand, technology-oriented standards prescribe (though often not mandatory) a specific technological solution to be applied. (Please note that a specific technological solution still does not promote a specific product or vendor.)

A summary of the comparison is presented in the following table.

Table 9.1 Characteristics of ISO 27043 and related standards

ISO standard	Area of concentration	Level of detail	Area of application	Technology oriented or process oriented?
27043 [21]	Principles and process; Complete digital forensic investigation process	High-level	Civil, criminal and enterprise investigations	Process oriented
27035-1 [101]	Incident management	High-level	Civil, criminal and enterprise investigations	Process oriented
27035-2 [102]	Incident response	Mid-level	Civil, criminal and enterprise investigations	Process and technology oriented
27035-3 [103]	CSIRT operations	Mid-level	Civil, criminal and enterprise investigations	Process and technology oriented
27037 [96]	Identification, collection, acquisition and preservation of digital evidence	Low-level	Civil, criminal and enterprise investigations	Process and technology oriented
27038 [97]	Digital redaction	Low-level	Digital redaction of documents	Technology oriented
27040 [98]	Storage security	Very low-level	Security of computer storage	Technology oriented
27041 [99]	Incident investigative method	High-level	Digital forensic methods, tools, processes and procedures	Process oriented
27042 [100]	Analysis and interpretation of digital evidence	High-level	Civil, criminal and enterprise investigations	Process oriented
27044 [104]	Security Information and Event management (SIEM)	Not clear, as standard is in early stages of development	Information and event management	Not clear, as standard is in early stages of development
27050 [105]	Electronic discovery	Mid-level	Identification, preservation, collection, processing, review and production of digital evidence	Process and technology oriented
30121 [106]	Digital forensic risk framework	High-level	Civil, criminal and enterprise investigations	Process oriented

The author now presents a comparison in terms of width of the standards (how wide the area of concentration and the area of application are) and in terms of depth of the standard (whether the standard provides high-level or low-level guidance). Note that this comparison is qualitative. The comparison is presented in the form of a graph and the scales have been scaled in the following manner:

- Standard’s width: 0 for narrow (covering one specific area) and 1 for wide (covering all areas of the digital forensic investigation process)
- Standard’s depth: 0 for high-level and 1 for low-level details

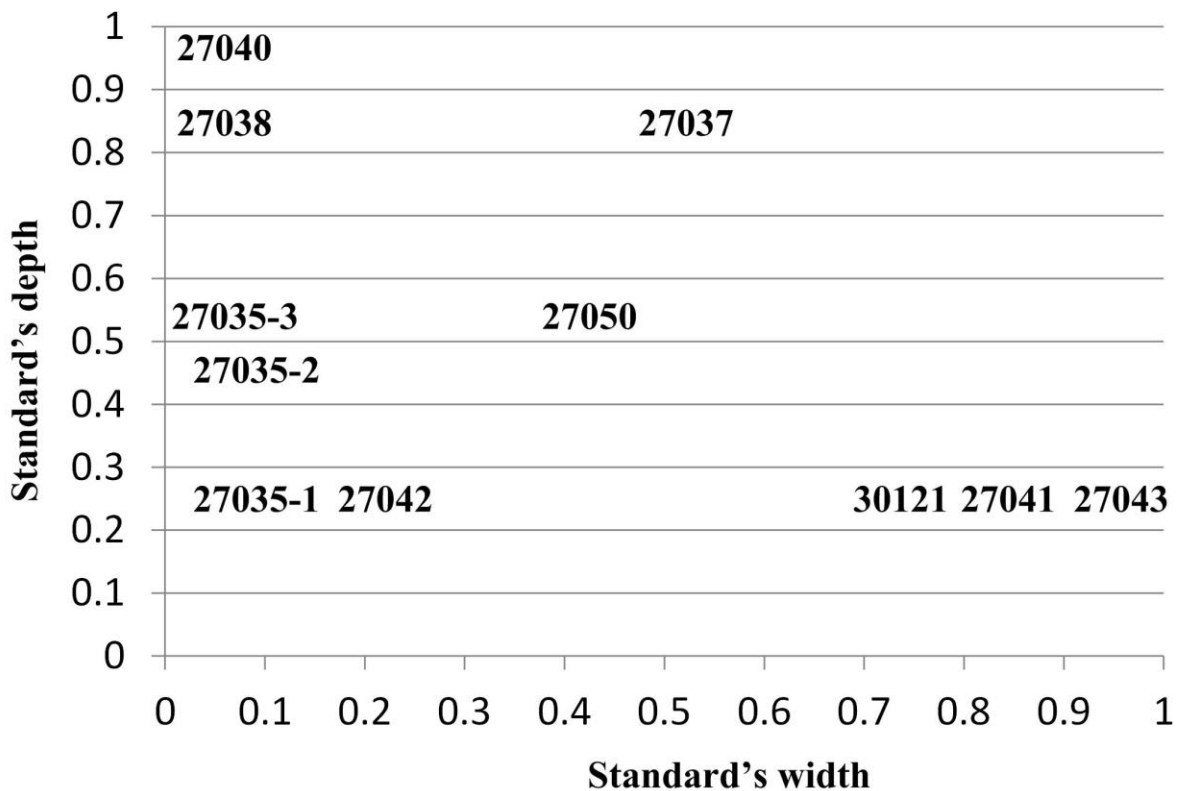


Figure 9.2 Comparing ISO 27043 and related international standards

Please note that the measures in the graph are qualitative and that they have been determined by the author based on an analysis of the above-mentioned parameters.

It is worthy to note that when compared to other high-level and “wide” standards, it is only ISO/IEC 27043:2015 [21] that concentrates on all aspects of digital forensic investigation. Others, such as 27041 [99] and 30121 [106], concentrate only on specific aspects of the digital forensic investigation process, namely methods and risk.

Based on the above, we can conclude that ISO/IEC 27043:2015 [21] is an overarching standard that applies to the field of the digital forensic investigation process. It represents the basis for the application of other related standards and is complemented by these related standards.

Based on the standard's width and depth, we can classify the analysed standards according to the classification presented in the following figure.

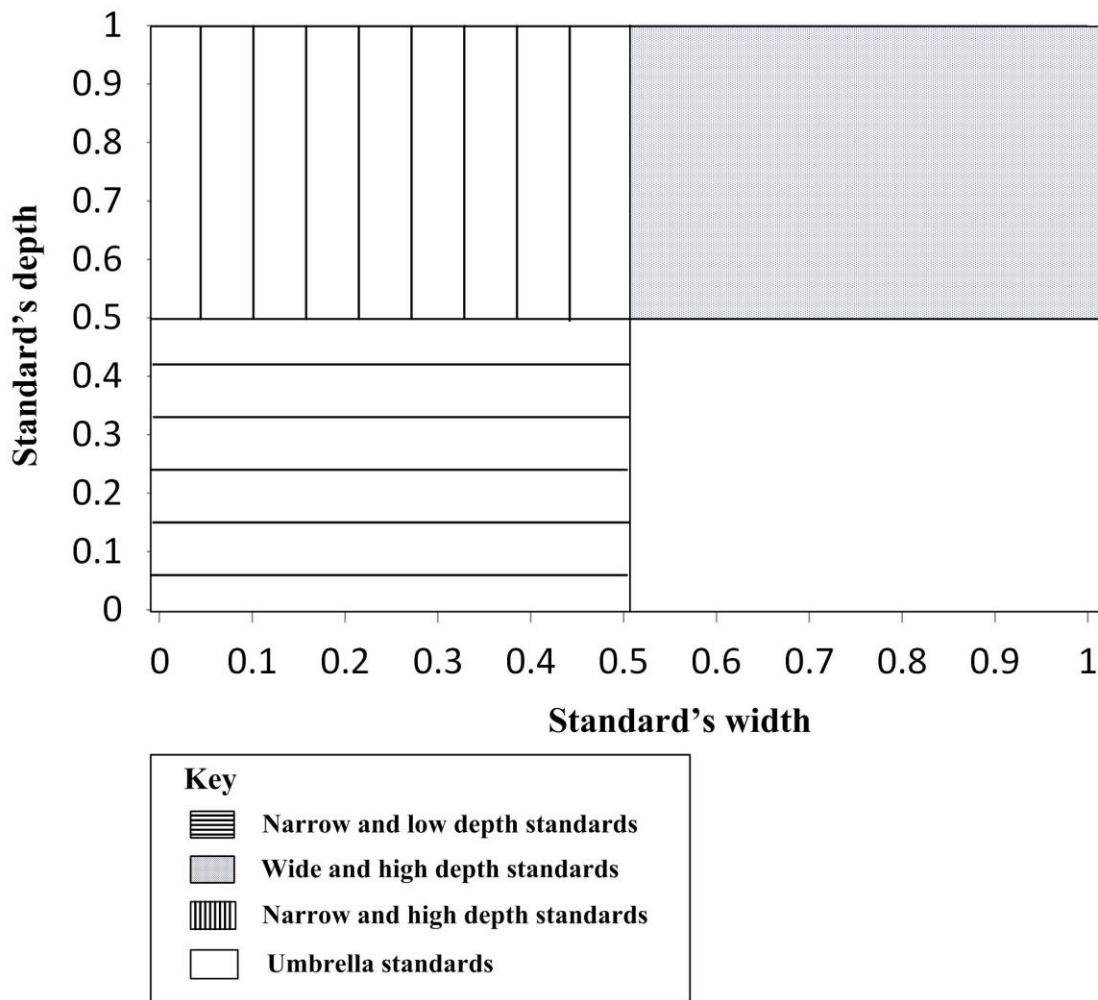


Figure 9.3 Classes of standards according to width and depth

Based on the standard's depth and width, we can classify them into one of the following categories:

- Narrow and low-depth standards
- Wide and high-depth standards
- Narrow and high-depth standards
- Umbrella standards (wide and low-depth standards)

Umbrella standards have width, but they do not contain a high level of detail. These standards are overarching and act as an “umbrella” when compared to other related standards.

Let us now take a look at how ISO/IEC 27043:2015 [21] and related standards fit into this classification.

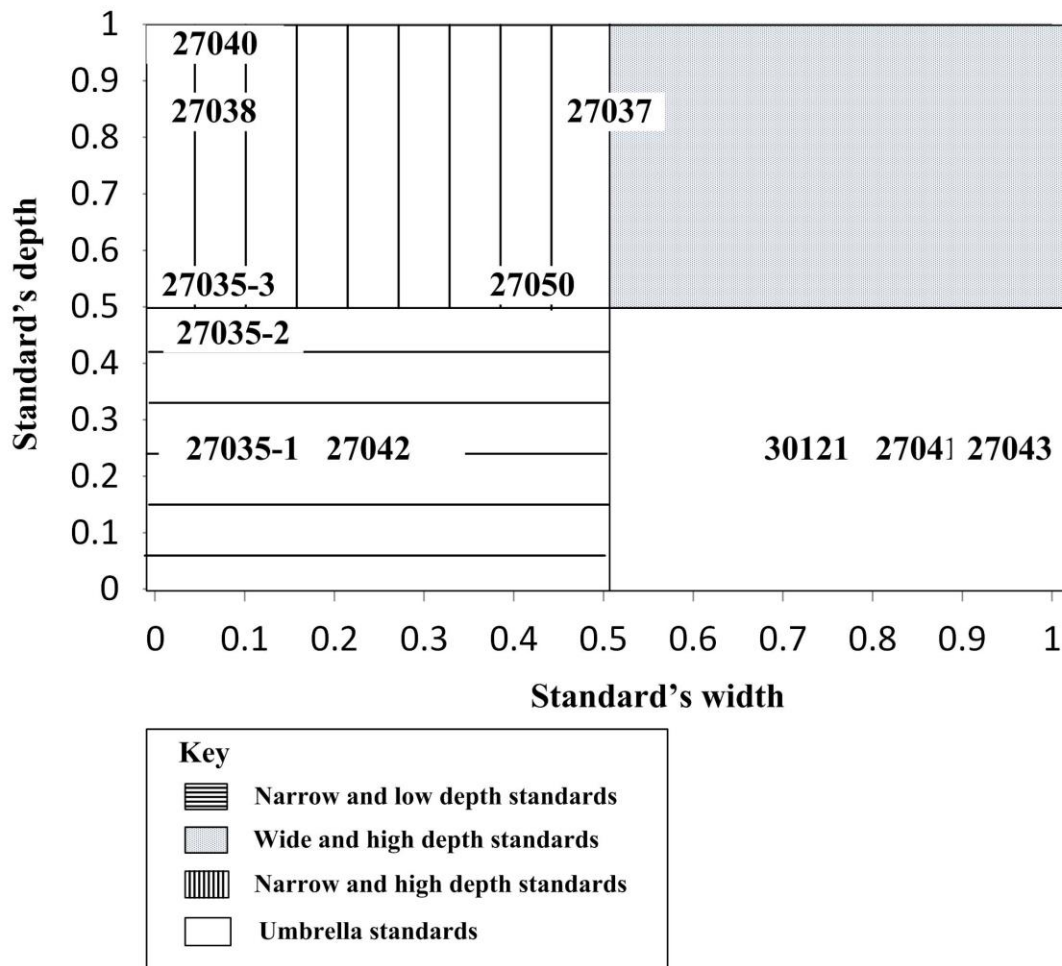


Figure 9.4 Classification of standards according to width and depth

We can conclude that ISO/IEC 27043:2015 is an “umbrella standard” with high width, thus it is comprehensive and clearly has a clear and unique position and role in the ecosystem with related standards.

9.5 Conclusion

In this chapter the author presented the ISO/IEC 27043:2015 international standard [21] and compared it with a number of related standards. **Chapter 9** enables the reader to understand the relations between the ISO/IEC 27043:2015 international standard [21] and related standards [96-106], as well as to understand the uniqueness, comprehensiveness and role of ISO/IEC 27043:2015 [21].

Next follows **Part 6** of the thesis. In this part the author discusses the proposed model and prototype and makes a critical evaluation of the contribution made by the thesis. **Part 6** also includes the conclusions chapter and outlines future work to be done.

PART 6: CONCLUSION

The first chapter in this part provides a critical evaluation of the contribution made by this thesis. The author discusses the proposed process model, the proposed prototype, and the results of testing the process model and prototype implementation. He furthermore analyses the extent to which the research problem has been solved and discusses the specific novelties introduced.

Chapter 11 concludes the thesis and provides indications of future work.

CHAPTER 10- CRITICAL EVALUATION

10.1 Introduction

In this chapter the author evaluates the extent to which the research problem has been addressed. He also evaluates and discusses the benefits, advantages, contributions and potential challenges of the proposed model and the prototype.

The section that follows provides a critical evaluation of the proposed model as the specific contribution of this research.

10.2 Critical evaluation of the proposed model

The problem addressed by this thesis is that by the start of writing of the thesis, there was a complete lack of a harmonised digital forensic investigation process model that could be used as a standardised set of guidelines for digital forensic investigations.

The proposed model represents a very significant step towards the harmonisation of existing models and towards achieving standardisation in the field. The harmonised model is comprehensive and introduces important novel approaches to the subject, such as *concurrent processes* and redefined and improved *readiness processes*, which represent important contributions. The proposed model, especially because of the above-mentioned novelties, enables efficient and effective digital forensic investigation, and also works towards increasing the admissibility of digital evidence in any court of law.

The proposed model should be used by scientists and practitioners in the field in their attempt to adopt a standardised digital forensic investigation process, improve digital evidence admissibility and solve collaboration issues.

Ultimately, the aim of the author is for the proposed model to be used for the standardisation of a digital forensic investigation process world-wide. The author launched an effort to standardise the process under the aegis of the International Standardization Organization [21]. The work presented in this thesis represents a significant input into the recently published international standard, ISO/IEC 27043:2015, “Information technology — Security techniques — Investigation principles and processes” [21]. The fact that this international standard was

published, with the author's work as major input, shows the high level of contribution of this thesis and the proposed model. During the editing and approval of the standard, the contributions presented in this thesis (which represent input into ISO/IEC 27043:2015) were critically evaluated by experts and practitioners, and eventually adopted as sound and valuable. These experts and practitioners included people from ISO working groups, professionals from different national standardisation bodies and independent experts from the field, who were all called upon to give their comments and inputs in respect of the proposed international standard [21].

The processes proposed in the model are well-defined in terms of scope, functions and order, which is an indication of the benefits and strengths of the contribution made. For the sake of simplicity of comprehension, the processes have also been grouped into process classes – an approach that carries the benefit of reduced complexity and ease of comprehension. This enabled the author to perform a functional grouping of processes, which in future can make it easier to introduce or change individual processes, seeing that no significant changes will have to be made to the model structure and organisation.

One of the process classes is distinctively different from the others. This particular class is concerned with achieving digital forensic investigation readiness for an organisation *before* an incident occurs, i.e. it is a proactive approach. The remainder of the process classes, however, follows a reactive approach. One should note that the proposed harmonised model includes the comprehensive class of readiness processes specifically to ensure that a holistic approach to the digital forensic investigation process is adopted and that is a significant contribution of this thesis. This holistic approach practically means that the implementation of these processes would enable the organisation to reap the benefits of cost and time efficiency and higher admissibility of digital evidence.

In the thesis the author also proposed several actions to be performed constantly and in parallel with the processes of the model so as to improve the efficiency of an investigation, ensure the admissibility of digital evidence, and promote collaboration. These actions are translated to *concurrent processes* that in turn translate the well-established principles into digital forensics such as preserving digital evidence and documenting actions. This is a novel approach and an important contribution to the digital forensic investigation process field. The application of these processes brings significant benefits.

Another important benefit involves the fact that the proposed model can be used across jurisdictions and across borders, due to the fact that it will ultimately be translated to an international standard. The model furthermore facilitates and promotes collaboration through specific processes such as the concurrent processes of *managing information flow* and *documentation*.

As explained above, the use of the proposed harmonised digital forensic investigation process model holds many benefits for digital forensic practitioners and academics. In summary, the benefits include the following:

- Higher admissibility of digital evidence in a court of law, due to the fact that a standardised process was used.
- Human error and omissions during the digital forensic investigation process would be minimised once such a harmonised process was introduced.
- Use of the proposed process model across national borders would enable modern society to fight cybercrime far more efficiently, and interaction between private and government entities would also be rendered much easier and more efficient.
- The proposed digital forensic investigation process model would enhance the efficiency and effectiveness of digital forensic investigations.
- Standardisation would be achieved in the field of digital forensic investigation process models.

As explained in earlier parts of this thesis, the proposed model was tested. Testing was performed on real-world cases and concentrated on examining the usability and effectiveness of the proposed model. The results showed that the proposed model could be successfully adapted to different types of digital forensic investigation. During testing it was concluded that the model facilitates improved admissibility of digital evidence and the results of digital forensic investigations, especially due to the introduction of the *concurrent processes* class.

The author recognises that there is a need to further improve the model by developing specific guidelines and procedures for specific types of investigation and enabling potential users to implement the proposed model in different types of digital forensic investigation

(cloud, live, mobile, network, etc.). For example, the *collection of digital evidence* process will be applied differently from a procedures and technology point of view in the case of a dead forensics, cloud forensics and mobile forensics case. However, defining these specific guidelines and procedures falls outside the scope of this thesis and should be included in future work.

Furthermore, the author recognises that the testing and evaluation of the proposed model should continue in the digital forensics community as a whole, especially to identify potential improvements and modifications to improve the model's ability to cater for all types of digital forensic investigation in an ever-changing environment.

It is recognised that challenges may arise when the proposed model is implemented in complex working environments with multiple parties and individuals involved, especially in respect of coordination and communication. It is further claimed that this challenge can be overcome if one adheres strictly to the implementation of the proposed concurrent processes, in particular the *documentation* process and the *managing information flow* process. The implementation of a specialised processes and tools can also assist. Such specialised process and tools can for example be from the fields of Enterprise Resource Planning (ERP), project management, human resources, case management, collection and analysis of digital evidence, data mining, etc.

Another part of the problem that this thesis addressed is that at the time of writing this thesis, there existed no prototype or software application for guidance through and implementation of a standardised digital forensic investigation process model that can be used as a standardised tool. The prototype proposed in the thesis addresses this problem by being a tool that can help investigators to adhere properly to a standardised digital forensic investigation process.

In next section the author makes critical evaluation of the proposed prototype software.

10.3 Critical evaluation of the proposed prototype

The proposed prototype is a significant step towards enabling implementation of a standardised digital forensic investigation process model. The prototype not only enables implementation, but also logging and non-repudiation of all user activities. It focuses especially on concurrent processes, which cater for evidence integrity.

The proposed prototype enables one to easily follow the standardised process, which results in higher admissibility of digital evidence and of the findings of digital forensic investigations. Higher admissibility is possible due to the fact that courts of law would probably be more satisfied when a standardised and formalised process was followed during a digital forensic investigation – a process that had passed significant peer review and had ultimately been accepted as an international standard.

The prototype could also be used for the training of novice investigators. Furthermore, the efficiency and effectiveness of digital forensic investigations could possibly be improved due to the fact that the prototype makes clear process guidelines available. Last, but not least, the prototype enables organisations to adopt the standardised process in a short period of time due to the training opportunity offered by the prototype.

The two main functionalities that provide the benefits as explained above, involve the model's acting as an expert system that can be used for guidance and training of novice investigators, and enabling the implementation of the investigation process while reliably logging all actions in a digital forensic fashion.

The author proposed a well-defined architecture for the prototype and defined key functional components, while taking into consideration information systems security. A web-based platform was chosen to develop the prototype so as to cater for multiple users from multiple locations and jurisdictions, with minimal requirements for client infrastructure. In addition to the characteristics of the model itself, this approach ensures easy collaboration between organisations and jurisdictions, independent of geographic location. This is of great importance in today's world where cybercrime and security incidents know no borders. A significant contribution involves the fact that the model and prototype together enable easier cross-jurisdictional, cross-border and cross-organisational cooperation when digital forensic

investigations are conducted, without requiring the setting up of specific hardware and software infrastructure for each of the involved parties.

Cryptography is used to ensure the confidentiality and integrity of all information, as well as to ensure the non-repudiation of user actions. This is an important aspect and a significant benefit as it ensures that the highest levels of information security are preserved, including information confidentiality and integrity.

The author acknowledges that further testing of the prototype is needed to test its full effectiveness and usability in different types of investigation and in different working environments. This will also help to detect any functional and technical faults, and improve the prototype with the ultimate aim of reaching a level of functionality and technical quality where practitioners can use the prototype in their work.

In next section the author revisits the research questions and objectives and he evaluates how successfully these have been addressed by the thesis.

10.4 Research questions

The research problem was subdivided into three research questions:

1. Can we achieve comprehensiveness and harmonisation of the digital forensic investigation process?
2. Can we achieve standardisation of the digital forensic investigation process?
3. Can we propose a software application prototype that would guide one through the implementation of a comprehensive and harmonised digital forensic investigation process, while at the same time validating the use of a proper process?

The author believes that he successfully answered all of the research questions as explained in detail in **Section 9.3**, as follows:

- Proposing a comprehensive and harmonised digital forensic investigation process;
- Contributing to the development of ISO/IEC 27043:2015 [21] international standard;
- Proposing the software prototype to assist with implementing the proposed process model.

It is important to note that the proposed model ultimately led to the standardisation of the processes used in digital forensic investigations and that the related standard [21] was published early in 2015.

The following section concludes the chapter.

10.5 Conclusion

In this chapter the author performed a critical evaluation of the proposed model and prototype in order to show the extent to which the research problem had been solved.

The author showed that the proposed model brings along significant benefits, which include harmonisation of the field, achieving comprehensiveness and, most importantly, accomplishing standardisation as well as higher admissibility, efficiency and effectiveness.

Furthermore, the proposed prototype ensures that the model is properly implemented and that implementation steps and conformance with requirements can be verified. This further strengthens the case for higher digital evidence admissibility and the improved efficiency and effectiveness of digital forensic investigations.

Both the model and the prototype can be used for conducting investigations, but also for the training of novice investigators. The model and the prototype furthermore enable cross-jurisdictional, cross-organisational and cross-border cooperation, which constitutes a significant benefit.

It can be concluded that the thesis as a whole represents a significant contribution to the field of digital forensics, as the proposed model has ultimately led to the publishing of an international standard [21]. Publications in journals and presentations at conferences

pertaining to the proposed model and prototype [107-113] also facilitated model's wide promotion and successful adoption.

The next chapter concludes the thesis, discusses the specific contributions made and gives an indication of planned future work.

CHAPTER 11- CONCLUSION

11.1 Introduction

This chapter concludes the thesis. The author provides a brief summary of the thesis, revisits the problem statement and emphasises specific contributions and benefits. This chapter also includes an indication of future work.

11.2 Revisiting the problem statement and research objectives

Let us revisit the problem statement. In the introductory chapter it was stated:

“When this thesis was being prepared, there existed neither an international standard for formalising the overarching digital forensic investigation process, nor a process model that was accepted as a harmonised model across different jurisdictions worldwide.”

The author therefore proposed a model that would be comprehensive and harmonised, and this model ultimately led to the standardisation in the field of digital forensic investigation processes.

The problem as stated was resolved through addressing each of the objectives set up for this thesis:

- The author first introduced the reader to the subject matter and studied relevant related work.
- He then proposed a digital forensic investigation process model that is comprehensive and harmonised.
- The author next compared the proposed model to existing models in order to verify the levels of comprehensiveness and harmonisation achieved.
- The proposed model was subsequently evaluated to determine its usability, adaptiveness, benefits and potential flaws.

- After that, a prototype software application for implementation of the proposed model was presented to help with providing guidelines and validating the use of the proposed process.
- The final objective of the study was that the proposed model should lead to the standardisation of the digital forensic investigation process, and this was achieved through engagement with the International Standardisation Organisation (ISO). The product of this engagement proved to be the published international standard ISO/IEC 27043:2015, “Information technology — Security techniques — Investigation principles and processes”.

As shown and explained above, all of the objectives were addressed and fully reached.

The following section provides a condensed chapter-by-chapter summary of the thesis. (Although the summaries may appear superfluous and repetitive (and may well be ignored), they are provided for the convenience of the reader and aim to improve the readability of the thesis.)

11.3 Thesis summary

In this section, all of the chapters are revisited and a brief summary of each is provided.

Chapter 1 provided an introduction to the research problem. The reader was introduced to subject of the thesis, after which the problem statement and research questions were defined. This chapter also discussed the motivation for the study and defined specific objectives.

Chapter 2 provided the reader with the background on digital forensics and digital forensics investigation processes, including digital forensic investigation readiness processes. This chapter also presented different types of digital forensic investigation. In this chapter the author also discussed related work that was used as a starting point in achieving harmonisation and comprehensiveness of the proposed process model.

Chapter 3 presented some background on legal requirements pertaining to digital forensics. Here the author presented relevant rules, guidelines and court cases, and discussed the need for a standardised digital forensic investigation process.

Chapter 4 presented the proposed comprehensive and harmonised digital forensic investigation process model.

Chapter 5 provided a comparison of the proposed model and existing models in order to better explain the proposed model's comprehensiveness and the harmonisation achieved.

Chapter 6 analysed the results of testing the proposed process model and then drew conclusions and presented findings regarding the process model's usability and effectiveness.

In **Chapter 7**, the author proposed a prototype that would guide an investigator through the implementation of a standardised and harmonised digital forensic investigation process.

Chapter 8 analysed the results of usability and effectiveness testing of the proposed prototype. Conclusions regarding prototype effectiveness and usability were also presented in this chapter.

Chapter 9 analysed ISO/IEC 27043:2015 international standard on digital forensic investigation process [21]. It also gave overview of related international standards and compared these to the international standard on digital forensic investigation process. Based on the comparisons made findings were made on ISO/IEC 27043:2015 [21] international standard's role, uniqueness and comprehensiveness.

Chapter 10 critically evaluated the contribution of the thesis and focused on discussing the proposed process, the proposed prototype, and the results of testing the process and prototype implementation in a real-world context. In this chapter the author also analysed the extent to which the research problem had been solved.

Chapter 11 concludes the thesis and provided indications of future research work.

The following section discusses the main contributions of the thesis and the novelties introduced.

11.4 Discussion on contributions and novelties

As shown in this and previous sections and chapters, the author successfully resolved the research problem, answered research questions and fulfilled research objectives. The ultimate aim of the study was the comprehensive harmonisation of the digital forensic investigation process model that is used to standardise the digital forensic investigation process. The specific contributions and novelties introduced by the proposed model include the following:

1. Harmonisation of existing state-of-the-art models, to enable cross-jurisdictional cooperation, to avoid human errors and omissions, and to facilitate the training of novice investigators.
2. Standardisation of the digital forensic investigation process implies a step even further than harmonisation. The use of a standardised process that ensures the integrity of digital evidence as well as the integrity of digital forensic investigation results and conclusions ultimately leads to higher admissibility of digital evidence in court and more effective and efficient investigations.
3. Introduction of the *concurrent processes* class facilitates more efficient investigations and higher admissibility of digital evidence through ensuring the integrity of both the digital evidence and the process that was followed. *Concurrent processes* also facilitate cooperation and collaboration. For example, *concurrent processes* ensure that an appropriate information flow is maintained between all stakeholders and also that each action is authorised by an appropriate person or authority.
4. Inclusion of the comprehensive *readiness processes* class into the model assists users to adopt a holistic approach and increase the effectiveness of investigations and admissibility of digital evidence, while also ensuring cost and time efficiency.
5. Enabling cross-jurisdictional, cross-border and cross-organisational cooperation helps users to investigate incidents that span across jurisdictions.

Specific contributions and novelties introduced by the proposed prototype software application include:

1. Easier implementation of the proposed model and thus more efficient investigations.
2. Validation of the digital forensic investigation process used, which increases the admissibility of digital evidence.
3. Cross-organisational, cross-border and cross-jurisdictional cooperation between organisations conducting digital forensic investigations.
4. Potential provision of the prototype software as Software-as-a-Service through a cloud platform, thus enabling users to concentrate on actual investigation activities.

The following section indicates future work.

11.5 Future research work

It is suggested that future work should include the development of more procedures to be included as guidelines for the implementation of the model in respect of different types of digital forensic investigation and different types of digital evidence. As the proposed model presents an “umbrella” for different types of digital forensic investigation (as explained in the thesis), it will be important in future to develop lower-level procedures and guidelines that will also include type-specific methodologies and even tools. For example, the *collection of potential digital evidence* process for post-mortem forensics and for mobile forensics would definitely use different sets of procedures and tools to collect potential digital evidence.

With regard to further work on the proposed prototype, a specific area identified for future research involves allowing for more structured inputs that would enable a shared interface with specialised software for digital evidence acquisition, analysis and interpretation, as well as with other specialised software in the field of digital forensics. In practice, the author envisages that the proposed prototype software should be able – without major development and integration efforts – to share an interface with specialised digital forensic investigation software available on the market, such as EnCase Forensic [114], Forensic Toolkit (FTK) [115] and The Sleuth Kit [116]. This should be achieved through assisting prototype software

to receive structured inputs, for example in a prescribed XML format or through a prescribed interface with different databases.

Moreover, future work should also concentrate on continuing with the evaluating and testing of the proposed model and the development of a model prototype. Tests and evaluations should be aimed at implementing the model and prototype in all of the different types of digital forensic investigation and under different circumstances (for example different operating systems on devices being investigated in mobile digital forensics cases, different types of cybercrime incidents, different hardware platforms, etc.). This should provide the opportunity to re-confirm the adaptability of the model and to identify areas where improvement and/or modification might be needed.

The author encourages the whole digital forensics community to take part in future work pertaining to this thesis, the proposed model and prototype, in order to allow for the full utilisation of benefits introduced in this thesis.

11.6 Final conclusion

The research reported on in this thesis has brought significant contributions and novelties to the field of digital forensics and in particular to the standardisation of the digital forensic investigation process. If applied on a large scale, the proposed process model and the prototype should certainly hold important benefits for the field. Last, but not least, the author hopes that both academics and practitioners will use this work to further advance and develop the field of digital forensic investigation.

REFERENCES

- [1] Wessels, “E-Inclusion: European Perspectives Beyond the Digital Divide”, University of Sheffield, UK, 2010
- [2] United States Presidents Information Technology Advisory Committee, “Report to the President Information Technology: Transforming our Society” [ONLINE], Available at https://www.nitrd.gov/pitac/report/section_1.aspx, , Accessed on 12 January 2015
- [3] Price Waterhouse Coopers, “The Global State of Information Security[®] Survey 2014”, Price Waterhouse Coopers, 2014
- [4] Microsoft, “Microsoft Security Intelligence Report Volume 17 | January through June, 2014”, 2014
- [5] Symantec, “Symantec Internet Security Threat Report 2014” [ONLINE], Available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf, Accessed on 12 March 2015
- [6] Ponemon Institute, “2014 Ponemon Cost of Cyber Crime study”, 2014
- [7] Center for Strategic and International Studies, “Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime”, McAfee, 2014
- [8] <http://www.linkedin.com/groups/Digital-Forensics-Association-DFA-36573/about>[ONLINE], Accessed on 20 February 2015
- [9] International Information Security South Africa Conference, <http://www.infosecsa.co.za/>
- [10] Security Research Institute (SRI) Security Congress, <http://scissec.scis.ecu.edu.au/>
- [11] Annual Forum of Incident Response and Security Teams (FIRST) Conference on Computer Security Incident Handling, <http://www.first.org/conference>

- [12] Annual International Federation for Information Processing (IFIP) Working Group (WG) 11.9 International Conference on Digital Forensics, <http://www.ifip119.org/Conferences/>
- [13] The International Conference on Availability, Reliability and Security (ARES), <http://www.ares-conference.eu/conference/>
- [14] International Workshop on Digital Forensics and Incident Analysis (WDFIA), <http://www.wdfia.org/>
- [15] The Association of Digital Forensics, Security and Law (ADFSL) Conference on Digital Forensics, Security and Law, www.adfsl.org
- [16] <http://www.enfsi.eu/> [ONLINE], Accessed on 20 July 2014
- [17] <http://www.ioce.org> [ONLINE], Accessed on 20 July 2014
- [18] <http://www.ifip119.org> [ONLINE], Accessed on 20 July 2014
- [19] Agrawal et al., “Systematic Digital Forensic Investigation Model”, International Journal of Computer Science Security, vol. 5, no. 1, 2011
- [20] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 1993
- [21] ISO/IEC 27043:2015, “Information Technology — Security Techniques — Investigation principles and processes”, international standard, 2015
- [22] *Trend Finance (Pty) Ltd and Another v Commissioner for the South African Revenue Service and Another (8712/01)*, ZAWCHC 55; [2005] 4 All SA 657 (C), 2005
- [23] *State v. Dunn*, 7 S.W.3d 427, 432 (Mo. Ct. App. 2000)
- [24] European Police Office, “Internet Organised Crime Threat Assessment (iOCTA) 2014”, 2014

- [25] Beebe, “Digital Forensic Research: The Good, the Bad and the Unaddressed”, *Advances in Digital Forensics V, IFIP Advances in Information and Communication Technology*, vol. 306, pp 17-36, 2009
- [26] Valjarevic and Venter, “Harmonized Digital Forensic Investigation Process Model”, *Proceedings of Information Security South Africa 2012 Conference*, 2012
- [27] Tan, “Forensic Readiness”, Technical. Cambridge USA: @stake, Inc., 2001
- [28] Dunham, “Mobile Malware Attacks and Defense”, Elsevier, 2009
- [29] McDougal, “Live Forensics on a Windows System: using Windows Forensic Toolkit (WFT)”, Fool Moon Software and Security, 2006
- [30] Jansen and Ayers, “Guidelines on Cell Phone Forensics”, National Institute of Standards and Technology Special publication 800-101, National Institute of Standards and Technology, U.S. Department of Commerce, 2006
- [31] Ruan et al., “Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: An Overview of Survey Results”, *Journal of Digital Investigation*, vol. 10, issue 1, June 2013, pp 34-43, 2013
- [32] Sibiya et al., “Digital Forensic Framework for a Cloud Environment”, *IST-Africa 2012 Conference Proceedings*, IIMC International Information Management Corporation, 2012
- [33] Ayers et al., “NIST Special Publication 800-101 Revision 1 Guidelines on Mobile Device Forensics”, National Institute of Standards and Technology, U.S. Department of Commerce, 2014
- [34] Olivier, “On Metadata Context in Database Forensics”, *Digital Investigation* 5.3–4, pp. 115-123, 2009
- [35] R v Aaron Caffrey, Southwark Crown Court, 2003
- [36] Brenner et al., “The Trojan Horse Defense in Cybercrime Cases”, *Santa Clara High Technology Law Journal*, Volume 21, Issue 1, Article 1, 2004

- [37] Ranum, “Network Forensics: Network Traffic Monitoring”, NFR Inc., 1997
- [38] SANS Digital Forensic and Incident Response Blog, “SQL, Databases and Forensics”, Available at: <http://digital-forensics.sans.org/blog/2009/03/11/sql-databases-and-forensics>, Accessed on 20 February 2015
- [39] Palmer, “A Road Map for Digital Forensic Research”, Technical Report DTR-T001-01, DFRWS, November 2001; Report from the First Digital Forensic Research Workshop (DFRWS), 2001
- [40] Reith et al., “An Examination of Digital Forensic Models”, International Journal of Digital Evidence, 2002
- [41] DOJ, the U.S. Department of Justice, “Electronic Crime Scene Investigation – a Guide for First Responders”, 2001
- [42] Carrier and Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, vol. 2, no. 2, [Electronic version], 2003
- [43] Mandia, Prosser and Pepe, “Incident Response & Computer Forensics” (Second Ed.), McGraw-Hill/Osborne, Emeryville, 2003
- [44] Beebe and Clark, “A Hierarchical, Objectives-Based Framework for the Digital Investigations Process”, Digital Investigation 2(2), 2005
- [45] Cuardhuain, “An Extended Model of Cybercrime Investigations”, International Journal of Digital Evidence, summer 2004, vol. 3, issue 1, 2004
- [46] Casey and Rose, chapter “Forensic Analysis ” in “Handbook of Digital Forensics and Investigation”, 2010, pp. 21-62
- [47] Cohen, “Fundamentals of Digital Forensic Evidence”, chapter in “Handbook of Information and Communication Security” [ONLINE], Available at all.net, Accessed on 04 January 2011
- [48] Carrier and Spafford, “An Event-Based Digital Forensic Investigation Framework”, Digital Investigation 2(2), 2005

- [49] Cohen, “Fundamentals of Digital Forensic Evidence”, chapter in “Handbook of Information and Communication security” [ONLINE], Available at all.net, Accessed on 04 January 2011
- [50] Pollitt, “Report on Digital Evidence”, 13th Interpol Forensic Science Symposium, France, 2001
- [51] ACPO, “ACPO Good Practice Guide for Computer-Based Evidence” [ONLINE], Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf , Accessed 18 February 2013
- [52] Yusoff et al., “Common Phases of Computer Forensics Investigation Models”, International Journal of Computer Science & Information Technology (IJCSIT), vol. 3, no. 3, 2011
- [53] Pollitt, “Computer Forensics: An Approach to Evidence in Cyberspace”, Proceeding of the National Information Systems Security Conference, Baltimore, MD, vol. II, 1995
- [54] Pollitt, “An Ad Hoc Review of Digital Forensic Models”, Proceeding of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE’07), Washington, USA, 2007
- [55] Baryamereeba and Tushabe, “The Enhanced Digital Investigation Process Model”, Proceeding of Digital Forensic Research Workshop, Baltimore, MD, 2004
- [56] Rogers et al., “Computer Forensic Field Triage Process Model”, presented at the Conference on Digital Forensics, Security and Law, 2006
- [57] Sundresan, “Digital Forensic Model based on Malaysian Investigation Process”, International Journal of Computer Science and Network Security, vol. 9, no. 8, 2009
- [58] Stephenson, "A Comprehensive Approach to Digital Incident Investigation", Information Security Technical Report, vol. 8, issue 2, 2003

- [59] Kohn et al. “Framework for a Digital Forensic Investigation”, Proceedings of the Information Security South Africa 2006 conference, 2006
- [60] Freiling and Schwittay, “Common Process Model for Incident and Computer Forensics”, in Proceedings of Conference on IT Incident Management and IT Forensics, Germany, 2007
- [61] Bem and Huebner, “Computer Forensic Analysis in a Virtual Environment”, International Journal of Digital Evidence, vol. 6, no. 2, 2007
- [62] Pilli et al. “Network Forensic Frameworks: Survey and Research Challenges”, Digital Investigation, vol. 7, 2010
- [63] Yasinsac and Manzano, “Policies to Enhance Computer and Network Forensics”; Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 2001
- [64] Wolfe-Wilson and Wolfe; “Management Strategies for Implementing Forensic Security Measures”, Information Security Technical Report, vol. 8, issue 2, 2003
- [65] Rowlingson, “A Ten Step Process for Forensic Readiness”; International Journal of Digital Evidence, 2004
- [66] Federal Rules of Evidence, U.S. Government Printing, 2010
- [67] Cybex, The Admissibility of Electronic Evidence in Court, Fighting Against High-Tech Crime (Cybex, Barcelona), 2005
- [68] Mason, “International Electronic Evidence”, British Institute of International and Comparative Law, 2008
- [69] Casey and Schatz, Chapter 6 in “Digital Evidence & Computer Crime”, 3rd edition, 2011
- [70] Maurer, “Modelling a Public-Key Infrastructure”, Computer Security—ESORICS 96, Springer, 1996

- [71] The Internet Engineering Task Force (IETF), “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)” [ONLINE], available at: <https://tools.ietf.org/html/rfc3161>, Accessed on 01 March 2015
- [72] Mumba and Venter, “Mobile Forensics Using the Harmonised Digital Forensic Investigation Process”, Proceedings of Information Security South Africa 2014 Conference, 2014
- [73] Micro Systemation (MSAB) XRY [ONLINE], Available at <http://www.msab.com>, Accessed on 20 February 2015
- [74] Omeleze and Venter, “Testing the Harmonised Digital Forensic Investigation Process Model Using an Android Mobile Phone”, Proceedings of Information Security South Africa 2013 Conference, 2013
- [75] Mumba and Venter, “Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Post Mortem Digital Investigations”, 2014 ADFSL Conference on Digital Forensics, Security and Law, 2014
- [76] www.android.com [ONLINE], Accessed 08 March 2015
- [77] global.blackberry.com [ONLINE], Accessed 08 March 2015
- [78] <http://windows.microsoft.com/en-ZA/windows/windows-help#windows=windows-7> [ONLINE], Accessed on 17 March 2015
- [79] <http://www.pcmag.com/encyclopedia/term/61745/sim-card> [ONLINE], Accessed on 17 March 2015
- [80] http://worldwide.blackberry.com/blackberrycurve/3G/curve_specifications.jsp [ONLINE], Accessed on 17 March 2015
- [81] Valjarevic, Venter and Ingles, “Towards a Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process”, Information Security South Africa 2014 conference proceedings/ IEEE Xplore Digital Library, 2014

- [82] Martin, “Rapid Application Development”, Macmillan, Indianapolis, IN, USA, 1991
- [83] “The world's most popular open source database” [ONLINE], Available at: <http://www.mysql.com/>, Accessed 03 November 2014
- [84] Dubey and Wagle, “Delivering Software as a Service”, The McKinsey Quarterly, 2007
- [85] PHP - Hypertext Preprocessor. 2014. *PHP: Hypertext Preprocessor* [ONLINE], Available at: <http://php.net/>, Accessed 03 November 2014
- [86] Laravel - The PHP framework for web artisans. 2014. *Laravel - The PHP framework for web artisans* [ONLINE], Available at: <http://laravel.com/>, Accessed 03 November 2014
- [87] Reenskaug and Coplien, “The DCI Architecture: A New Vision of Object-Oriented Programming” [ONLINE], 2009, Available at http://www.artima.com/articles/dci_vision.html, Accessed on 20 February 2015
- [88] Burbeck, “Applications Programming in Smalltalk-80(TM): How to use Model-View-Controller (MVC)” [ONLINE], 1992, Available at <http://www.math.sfedu.ru/smalltalk/gui/mvc.pdf>, Accessed on 20 February 2015
- [89] Sentry Manual - Cartalyst. 2014. *Sentry Manual Cartalyst* [ONLINE], Available at: <https://cartalyst.com/manual/sentry>, Accessed 03 November 2014
- [90] Wkhtmltopdf 2014. *wkhtmltopdf* [ONLINE], Available at: <http://wkhtmltopdf.org/>, Accessed 03 November 2014
- [91] Qt WebKit | QtWebKit 5.3 | Documentation | Qt Project. 2014. *Qt WebKit | QtWebKit 5.3 | Documentation | Qt Project* [ONLINE], Available at: <http://qt-project.org/doc/qt-5/qtwebkit-index.html>, Accessed 05 November 2014
- [92] NitMedia/wkhtml2pdf – GitHub 2014 [ONLINE], Available at <https://github.com/NitMedia/wkhtml2pdf>, Accessed 03 November 2014

- [93] http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm [ONLINE], Accessed on 20 February 2015
- [94] “Federal Information Processing Standards Publication 197 November 26, 2001 Announcing the ADVANCED ENCRYPTION STANDARD (AES)”, National Institute of Standards and Technology, U.S. Department of Commerce, 2001
- [95] <http://sumi.ucc.ie/> [ONLINE], Accessed 08 January 2015
- [96] ISO/IEC 27037:2012, “Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence”, international standard, 2012
- [97] ISO/IEC 27038:2014, “Information technology -- Security techniques -- Specification for digital redaction”, international standard, 2014
- [98] ISO/IEC 27040:2015, “Information technology -- Security techniques -- Storage security”, international standard, 2015
- [99] ISO/IEC FDIS 27041, “Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method”, unpublished final draft international standard, 2015
- [100] ISO/IEC DIS 27042, “Information technology -- Security techniques -- Guidelines for the analysis and interpretation of digital evidence”, unpublished draft international standard, 2015
- [101] ISO/IEC CD 27035-1, “Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management”, unpublished draft international standard, 2015
- [102] ISO/IEC CD 27035-2, “Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response”, unpublished draft international standard, 2015

- [103] ISO/IEC CD 27035-3, “Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations”, unpublished draft international standard, 2015
- [104] ISO/IEC WD 27044, “Guidelines for Security Information and Event Management (SIEM)”, unpublished working draft international standard, 2015
- [105] ISO/IEC CD 27050-1, “Information technology -- Security techniques -- Electronic discovery -- Part 1: Overview and concepts”, unpublished draft international standard, 2015
- [106] ISO/IEC 30121:2015, “Information technology -- Governance of digital forensic risk framework”, international standard, 2015
- [107] Valjarevic and Venter, “Towards Digital Forensic Readiness Framework for Public Key Infrastructure Systems”, Information Security South Africa 2011 conference proceedings/ IEEE Xplore Digital Library, 2011
- [108] Valjarevic and Venter, “Harmonised Digital Forensic Investigation Process Model”, International workshop on Digital Forensics in the Cloud (IWDFC)/ Information Security South Africa 2012 conference proceedings / IEEE Xplore Digital Library, 2012
- [109] Valjarevic and Venter, “Analyses of the State-of-the-art Digital Forensic Investigation Process Models”, The Southern Africa Telecommunication Networks and Applications Conference (SATNAC) proceedings, 2011
- [110] Valjarevic and Venter, “Towards a Harmonized Digital Forensic Investigation Readiness Process Model”, Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics proceedings/Advances in Digital Forensics, 2013
- [111] Valjarevic and Venter, “Implementation Guidelines for a Harmonised Digital Forensic Investigation Readiness Process Model”, Information Security South Africa 2013 conference proceedings/ IEEE Xplore Digital Library, 2013

- [112] Valjarevic, Venter and Ingles, “Towards a Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process”, Information Security South Africa 2014 conference proceedings/ IEEE Xplore Digital Library, 2014
- [113] Valjarevic and Venter, “A Comprehensive and Harmonized Digital Forensic Investigation Process Model”, Journal of Forensic Sciences, accepted, to be published in September 2015
- [114] <https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx> [ONLINE], Accessed 20 February 2015
- [115] <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk> [ONLINE], Accessed 20 February 2015
- [116] <http://www.sleuthkit.org/> [ONLINE], Accessed 20 February 2015
- [117] ISO/IEC 12207:2008, “Systems and software engineering -- Software life cycle processes”, international standard, 2008
- [118] <http://www.businessdictionary.com/definition/harmonization.html#ixzz3VKmEpZtu> [ONLINE], Accessed 26 March 2015
- [119] ISO/IEC 27000:2014, “Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary”, international standard, 2014
- [120] ISO 9000:2005, “Quality management systems -- Fundamentals and vocabulary”, international standard, 2005
- [121] ISO/IEC 27004:2009, “Information technology — Security techniques — Information security management — Measurement”, international standard, 2009

APPENDIX A- LIST OF RELATED WORK PUBLISHED BY THE AUTHOR

- Valjarevic and Venter, “Towards Digital Forensic Readiness Framework for Public Key Infrastructure Systems”, Information Security South Africa 2011 conference proceedings/ IEEE Xplore Digital Library, 2011
- Valjarevic and Venter, “Towards Solving the Identity Challenge Faced by Digital Forensics”, 7th International Annual Workshop on Digital Forensics & Incident Analysis (WDFIA 2012) proceedings, 2012
- Valjarevic and Venter, “Harmonised Digital Forensic Investigation Process Model”, International workshop on Digital Forensics in the Cloud (IWDFC)/ Information Security South Africa 2012 conference proceedings / IEEE Xplore Digital Library, 2012
- Valjarevic and Venter, “Analyses of the State-of-the-art Digital Forensic Investigation Process Models”, The Southern Africa Telecommunication Networks and Applications Conference (SATNAC) proceedings, 2011
- Valjarevic and Venter, “Towards a Harmonized Digital Forensic Investigation Readiness Process Model”, Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics proceedings/Advances in Digital Forensics, 2013
- Valjarevic and Venter, “Implementation Guidelines for a Harmonised Digital Forensic Investigation Readiness Process Model”, Information Security South Africa 2013 conference proceedings/ IEEE Xplore Digital Library, 2013
- Valjarevic, Venter and Ingles, “Towards a Prototype for Guidance and Implementation of a Standardized Digital Forensic Investigation Process”, Information Security South Africa 2014 conference proceedings/ IEEE Xplore Digital Library, 2014
- Valjarevic and Venter, “A Comprehensive and Harmonized Digital Forensic Investigation Process Model”, Journal of Forensic Sciences, accepted, to be published in September 2015
- Valjarevic and Venter, “Introduction of Concurrent Processes into the Digital Forensic Investigation Process”, Australian Journal of Forensic Sciences, accepted, to be published in May 2016

APPENDIX B- TERMS AND DEFINITIONS

For the purposes of this thesis, the following terms and definitions apply. These terms and definitions are mostly copied directly from ISO/IEC 27043:2015 standard [21]. [SOURCE] field defines the source of the term or definition as given in ISO/IEC 27043:2015 standard [21]. Furthermore, note that each of these sources has been referenced in the *References* section above.

acquisition

process of creating a copy of data within a defined set

Note: The product of an acquisition is a potential digital evidence copy.

[SOURCE: ISO/IEC 27037:2012 [96], 3.1]

activity

set of cohesive tasks of a process

[SOURCE: ISO/IEC 12207:2008 [97], 4.3]

analysis

process of evaluating potential digital evidence in order to assess its relevance to the investigation

Note: Potential digital evidence that is determined to be relevant, becomes digital evidence.

[SOURCE: ISO/IEC 27042 [98]:—, 3.1]

collection

process of gathering the physical items that contain potential digital evidence

[SOURCE: ISO/IEC 27037:2012 [96], 3.3]

digital evidence

information or data, stored or transmitted in binary form, that may be relied on as evidence

[SOURCE: ISO/IEC 27037:2012 [96], 3.5]

digital investigation

use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return and/or destruction of digital evidence derived from digital sources, while obtaining proper authorisations for all activities, properly documenting all activities, interacting with the physical investigation, preserving digital evidence and maintaining the chain of custody, for the purpose of facilitating or furthering the reconstruction of events found to be incidents requiring a digital investigation, whether of criminal nature or not [21]

harmonisation

For the purpose of this thesis harmonisation can be defined as: “adjustment of differences and inconsistencies among different processes to make them uniform, mutually compatible and more effective.” This is modification, for the purpose of this thesis and the research subject, of the definition presented in Business Dictionary [118].

identification

process involving the search for, recognition and documentation of potential digital evidence

[SOURCE: ISO/IEC 27037:2012 [96], 3.12]

incident

single or a series of unwanted or unexpected information security breaches or events, whether of criminal nature or not, that have a significant probability of compromising business operations or threatening information security [21]

interpretation

synthesis of an explanation, within agreed limits, for the factual information about evidence resulting from the set of examinations and analysis making up the investigation

[SOURCE: ISO/IEC 27042 [98]:—, 3.9]

investigation

application of examinations, analysis and interpretation to aid understanding of an incident

[SOURCE: ISO/IEC 27042 [98]:—, 3.10]

method

definition of an operation which can be used to produce data or derive information as an output from specified inputs

[SOURCE: ISO/IEC 27041 [99]:—, 3.11]

potential digital evidence

information or data, stored or transmitted in binary form which has not yet been determined through the process of examination and analysis to be relevant to the investigation

[SOURCE: ISO/IEC 27042 [98]:—, 3.15, modified – definition adapted to refer to the abstract process ‘examination and analysis’ rather than analysis only; note 1 and note 2 to entry not included]

preservation

process to maintain and safeguard the integrity and/or original condition of the potential digital evidence and digital evidence

[SOURCE: ISO/IEC 27037:2012 [96], 3.15, modified – added ‘and digital evidence’]

process

set of activities that have a common goal and last for a limited period of time

Note 1: Also see ISO/IEC 27000:2014 [119] and ISO 9000 [120] for similar definitions of a process.

Note 2: The concept ‘process’ in this thesis refers to a higher level of abstraction than the definition of ‘process’ in ISO/IEC 27041 [99].

Note 3: The term ‘phase’ is used by some of the authors of related works as a synonym for the term ‘process’.

readiness

the process of being prepared for a digital investigation before an incident has occurred [21]

validation

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[SOURCE: ISO/IEC 27004:2009 [121], 3.17]

verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

Note: Verification only provides assurance that a product conforms to its specification.

[SOURCE: ISO/IEC 27041 [99]:—, 3.20]

volatile data

caused by data that is especially prone to change and can be easily modified

[SOURCE: ISO/IEC 27037:2012 [96], 3.26, modified – inserted ‘caused by’ at the beginning of the original definition]

APPENDIX C- LIST OF ABBREVIATIONS

The following table describes the meaning of abbreviations and acronyms used throughout the thesis. The page on which each one is defined or first used is also given.

Abbreviation	Meaning	Page
ACPO	Association of Chief Police Officers	24
AEEC Project	Admissibility of Electronic Evidence in Court Project	32
CIA	Confidentiality, Integrity, Availability	41
DDoS	Distributed Denial of Service	17
DFI	Digital Forensic Investigation	29
DFIP	Digital Forensic Investigation Process	2
DFIRP	Digital Forensic Investigation Readiness Process	28
DOJ	Department of Justice	20
DFRWS	Digital Forensic Research Workshop	19
DVD	Digital Video Disc	85
EC3	European Cybercrime Centre	5
ENFSI	European Network of Forensic Science Institutes	3
ERD	Entity Relation Diagrams	18
FTK	Forensic Toolkit	97
HTML	HyperText Markup Language	105
ICCID	Integrated Circuit Card Identifier	89

Abbreviation	Meaning	Page
ICSA	Information and Computer Security Architecture research group of the Computer Science Department at the University of Pretoria	84
IDS	Intrusion Detection System	28
IMEI	International Mobile Equipment Identity Number	87
IMSI	International Mobile Subscriber Identity	89
IQR	Interquartile Range	125
iOCTA	Internet Organised Crime Threat Assessment	5
ISO	International Standardization Organization	4
JPEG	Joint Photographic Expert Group	34
MMS	Multimedia Message Service	89
MVC	Model-View-Controller	105
PC	Personal Computer	17
PDF	Portable Document Format	105
PKI	Public Key Infrastructure	61
RAD	Rapid Application Development	104
RAM	Random Access Memory	17
REST	Representational State Transfer	105
SaaS	Software as a Service	105
SD	Secure Digital Memory	88
SIM	Subscriber Identity Module	85
SMS	Secure Message Service	88

Abbreviation	Meaning	Page
SUMI	Software Usability Measurement Inventory	124
XML	Extensible Markup Language	113

APPENDIX D- USER GUIDE FOR A PROTOTYPE FOR THE GUIDANCE AND IMPLEMENTATION OF A STANDARDISED DIGITAL FORENSIC INVESTIGATION PROCESS

In this Appendix the author presents a user guide to accompany the prototype software proposed in this thesis. The user guide was developed by the author and fellow students from the ICSA research group at the University of Pretoria, for the purpose of guiding users during the testing and evaluation of the prototype.

The software prototype is available online, as explained in the provided user guide. If an interested party wishes to access the prototype, log-in credentials will be needed. Anyone who is interested to access the prototype is invited to send an email to:

alex@forensic-guidance.co.za



**Guidance and Implementation
of Standardized Digital Forensic
Investigation Process**

DFG USER MANUAL

Manual for the online Digital Forensic Guidance
software

Authors: Melissa Ingels and Aleksandar Valjarevic
Information and Computer Security Architecture Research Group
Department of Computer Science
University of Pretoria

Contents

Introduction.....	184
User roles	185
Software access.....	186
Log-in.....	187
Choosing a project	188
Implementing a step.....	189
Closing and reopening steps	191
Viewing and printing process guidance.....	192
Logs.....	193
Reports	194
Admin	195
User management.....	195
Organization management	195
Project management.....	196

Introduction

The Digital Forensic Guidance software is a prototype for guidance and implementation of the standardized digital forensic investigation process model. The software has two main functionalities:

- The first functionality would be to act as an expert system that can be used for guiding and training of novice investigators.
- The second main functionality would be to enable the implementation of the investigation process while reliably logging all actions in a digital forensic sound manner. Ultimately, the latter functionality would enable the validation of use of a proper digital forensic investigation process.

The use of the software would significantly help any organization involved with digital forensic investigations to follow a standardized process and improve admissibility of digital evidence and results of investigations. Also, the software can be used by organizations involved with or providing training in the field.

User roles

The following user roles are provided:

- System Overseer - This role has access to implementing all steps as well as closing and reopening of all steps. This role is also allowed to generate reports for the organization the user is part of, reports for all users inside the organization as well as all reports for the projects the user is allowed to access.
- System Owner - This role has access to implementing all steps as well as access to the admin part of the application
- System Custodian - This role has access to implementing all steps of the *Readiness processes class*
- System Administrator - This role has access to implement all steps of the *Readiness processes class* after the “*Implementing system architecture*” step.
- First Responder - This role has access to implementing all steps of the *Initialization processes class* as well as all steps of the *Acquisitive processes class*.
- Investigator - This role has access to implementing all steps of the *Initialization processes class*, all steps of the *Acquisitive processes class* as well as all steps of the *Investigative process class*.
- Analyst - This role has access to implementing all steps of the *Initialization processes class*, all steps of the *Acquisitive processes class* as well as all steps of the *Investigative process class*.
- Legal System Representative - This role has access to generating reports only
- Accused - This role has access to generating reports only

Software access

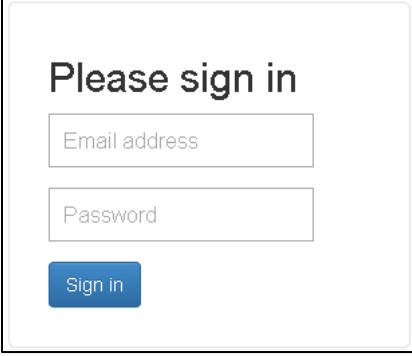
To access the software please visit <http://www.forensic-guidance.co.za>

Before using this software

- i. Your organization has to be registered on the software, an organization can be registered by sending a request to alex@forensic-guidance.co.za
- ii. Your System Owner (person who registered the organization) has to register the users that will be using the software and assign roles to them (see User Management).
- iii. In order to use this software you have to be registered.
- iv. In order to complete any of the steps on the software you will need a digital certificate to sign documents with. The System Owner can generate a digital certificate for you from the admin page.

Log-in

- i. When you encounter the log-in page, enter the log-in details provided to you by your System Owner.



Please sign in

Email address

Password

Sign in

- ii. If log-in fails you will receive an error message, if log-in succeeds you will be redirected to the project selecting page.

Choosing a project

- i. Once you have logged in you will be able to choose a project to load. If no projects are displayed it means you have not yet been added to any of the projects.
- ii. After selecting a project you will be shown to the main site. Here you can choose a step to implement, log out or (if you are the system owner) access the admin page.

Choose project

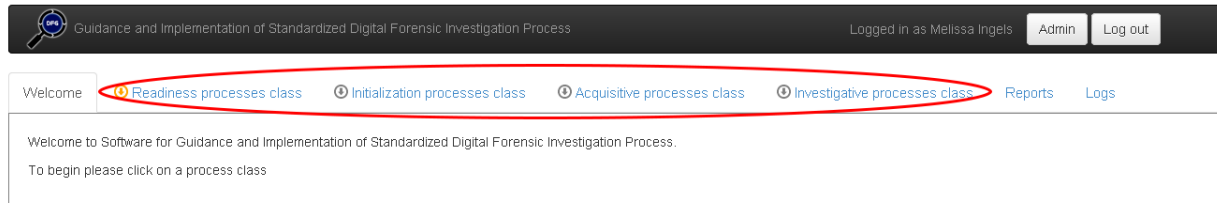
Project A

Project B

Project C

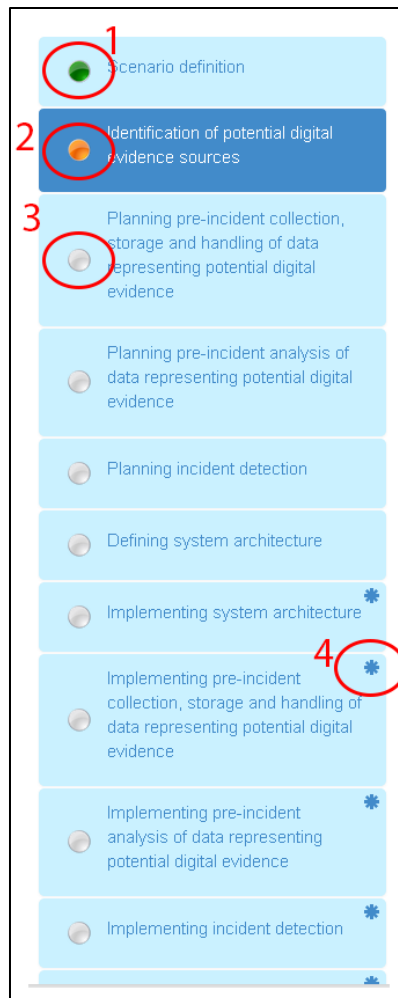
Implementing a step

- i. To start implementing a step, you will have to select a process class first. A process with an orange down arrow has steps that can be implemented. Processes with grey down arrows cannot yet be implemented and processes with green down arrows are completed.



- ii. After selecting the process class you want to implement you can select a step to implement. Steps dot color meanings are as follows:
 - a. Green dots – Completed (1)
 - b. Orange dots – In progress (2)
 - c. Grey dots – Cannot be implemented yet. (3)

Steps with a blue star (4) on the right means you have permission to implement this step.



- iii. Once you have selected a step that you have permission to implement, you will need to fill in the information to the right. All uploaded documents have to be digitally signed by the certificate provided to you by your System Owner.

The screenshot shows a web form titled "Data Inputs" with a "Close Step" button in the top right corner. The form is divided into two main sections: "Data Inputs" and "Concurrent processes".

Data Inputs Section:

- Potential digital evidence sources document:** A box containing a "Choose File" button and the text "No file chosen".
- Additional Documents:** A box containing a "Choose File" button and the text "No file chosen".

Concurrent processes Section:

- Obtaining authorization:** A box containing "Authorization documents" with a "Choose File" button and "No file chosen".
- Documentation:** A box containing "Documentation" with a "Choose File" button and "No file chosen".
- Managing information flow:** A box containing:
 - Name:** A text input field.
 - Encryption/security measures used:** A text input field.
 - Information flow document:** A "Choose File" button and "No file chosen".

At the bottom of the form, there are two buttons: "Close Step" and "Next".

- iv. Submitting a step will upload the data to the server, however to proceed your System Overseer has to close the step (See Closing and reopening steps)

Closing and reopening steps

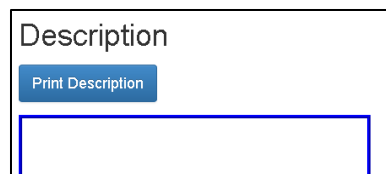
- i. Closing a step prevents data from being uploaded to that step. A step has to be closed in order to proceed to the next step.
- ii. Reopening a step allows data to be uploaded to that step, all subsequent steps are also reopened. The process flow will have to be followed again.

Viewing and printing process guidance

- i. To view process guidance, click on one of the buttons shown below. One button will have the current process name printed on it (1) and will display the model for that process class. The other button (2) will display the complete Standardized digital forensic investigation model.



- ii. Once you open the model you will be able to view it as well as print it, by clicking on the print button, next to the close button.



- iii. You can also print the step description by clicking on the print description button

Logs

- i. On each step that you have permission to implement there will be a logs table at the bottom.
- ii. The logs table shows the data that was uploaded for this step, it will show the user entered data as well as provide a download link for the files that were uploaded.
- iii. You can also view logs from the logs tab, this will show the logs for all the steps you have permission to implement

Logs				
Step name	User Email	User data	File	Date
Scenario definition name	peppercat101@gmail.com	Definition 1		2014-08-28 09:52:24
Scenario definition document	peppercat101@gmail.com		Download	2014-08-28 09:52:24
Risk assessment document	peppercat101@gmail.com		Download	2014-08-28 09:52:24
Additional Documents	peppercat101@gmail.com		Download	2014-08-28 09:52:25

Reports

- i. Users with the appropriate permissions can generate and download the following reports by going to the report tab and selecting the report they want to generate.
 - a. Complete compliance report – This report can be used in court to confirm that the proper process was followed during the investigation for the project. This report includes an overview of all the data uploaded, including information on when and by whom it was uploaded. It also shows iterations (when a step was closed and reopened).
 - b. User report- This report shows the roles as well as a summary of steps completed by the user within a selected time frame.
 - c. Organization report – This report shows the projects that were completed or are in progress for the certain organization within a selected timeframe. It also shows a summary of the users as well as the steps completed for each project.
 - d. Project report – This report shows a summary of steps as well as a summary of the users who worked on it for the selected project.

Admin

User management

- i. In the user view of the admin section the following actions can be done:
 - a. Adding a user- Adding a user will automatically add that user to the organization of the currently logged on user. While adding the roles for the user can also be selected.
 - b. Editing a user – Here the first name, last name and roles of the user can be changed. The password and email cannot be changed.
 - c. Deleting a user – Deleting a user will disable the user account but will not delete the user from the database as the user information can still be included in the reports and logs.
 - d. Generate certificate – This will generate a digital certificate for the selected user in order for him to sign the documents he uploads to the server. When a certificate is generated the current user will be redirected to a page with a download link for the certificate, a password to import the certificate with as well as the private key corresponding to the certificate. This information gets destroyed after 10 minutes. It will be the responsibility of the currently logged in user to decide how to give the information to the appropriate user.

Organization management

- i. In this view the following actions can be preformed
 - a. Add/Remove - When a user is removed from an organization his account will be disabled and he will not be allowed to log in. If the user is then added to an organization again, his account will be re-enabled. Only users that are not currently in an organization can be added to an organization.
 - b. Edit organization – Editing an organization allows you to change the name as well as which other organizations are allowed to see your users. Organizations that are allowed to see your users, cannot edit them but they can add them to projects. This is useful if two organizations work on the same project.
- ii. An organization can only be added or deleted by the software host via a request from the organization.

Project management

- i. In this view the following actions can be preformed
 - a. Add a project - You can enter a name and case number for the project
 - b. Edit a project – You can change the name and case number of the project
 - c. Add/Remove users – Users can be added or removed from the selected project, users that can be added are users in the current organization or users from organizations that gave permission for this organization to see their users.
 - d. Close/Reopen project – A project can be closed and reopened, closing a project does not delete the project but prevents any actions on the project, the project will not appear in the project selection page. Reopening a project will display it again.
- ii. A project cannot be deleted

APPENDIX E- SOURCE CODE FOR THE PROTOTYPE FOR GUIDING AND IMPLEMENTING A STANDARDISED DIGITAL FORENSIC INVESTIGATION PROCESS

Due to its size, source code is attached in electronic form.

What follows is a brief overview of the system architecture from a coding point of view and explanation of the attached electronic form of the source code.

Database

The database is implemented using MySQL. The database architecture and relationships were generated using the built-in migration offered by Laravel.

Language and Framework

The prototype is implemented using the PHP coding language and the Laravel Framework. The Blade templating engine was used for handling the views.

User management

Sentry was used for user management. Sentry is an add-on to Laravel.

Report generator

For generating reports, the tool wkhtmltopdf was used. wkhtmltopdf is an open source command-line tool to render HTML into PDF using the QT Webkit rendering engine. The NitMedia wrapper was selected to use the tool easily within Laravel. This wrapper converts the normal wkhtmltopdf package into a composer package that is usable in the Laravel framework. The reports are first generated in an html page using the Blade engine, the html is then passed to wkhtmltopdf and the resulting pdf document can be streamed to the browser. The reports were made to run in the background, because reports on big projects take long to generate (seeing that all the data has to be decrypted). To support the background process, we used Iron MQ, a reliable messaging queue. Laravel already has Iron MQ support.

Libraries and add-ons

Libraries and add-ons are managed using Composer. Composer is a tool for managing and installing PHP dependencies. Libraries are specified in the `Composer.json` file. When composer is run through the command line, it downloads all the required libraries using the specified version. For a full list of dependencies and libraries used, please see the `composer.json` file.

Theme

For the User Interface theme, Twitter bootstrap was used. Bootstrap is an open-source framework for developing responsive websites.

Source code files

Files under the following directories contain code written for the purpose of this research:

“App/classes” – Custom classes. Includes Encryption and Message queue response class, as well as multiple classes used to facilitate the process of generating a report.

“App/Controllers” – Includes all controllers for the software.

“App/database/seeds” –Includes classes created for seeding data into the database.

“App/models” – Includes all the models used in the software. Laravel gets all the fields and types automatically from the database. These models specify the table to be used and include functions used for extra processing before or after data is sent or received from the database.

“App/Views” – Includes all the files used for views. Most of the files make use of the Blade templating engine. Files under the widget directory are bits of the view that were reused in multiple places to minimise the repetition of code.

“public” – Files under the “public” directory range from css files, javascript files, as well as images and pdfs.

The rest of the files in the source code were either included in the Laravel framework, generated automatically or downloaded by using composer.

***APPENDIX F– ELECTRONIC COPY OF THE SOURCE CODE FOR THE
PROTOTYPE FOR GUIDING AND IMPLEMENTING A STANDARDISED
DIGITAL FORENSIC INVESTIGATION PROCESS***

An electronic copy of the source code for the prototype proposed for the guidance and implementation of a standardised digital forensic investigation process is attached as **Appendix F**.