

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS  
MODEL FOR EVIDENTIARY DATA HANDLING**

by

EL ANTONIO POOE

submitted in accordance with the requirements  
for the degree of

DOCTOR OF PHILOSOPHY

in the subject

INFORMATION SYSTEMS

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF. L. LABUSCHAGNE

MAY 2018

## ABSTRACT

---

There is a growing global recognition as to the importance of outlawing malicious computer-related acts in a timely manner, yet few organisations have the legal and technical resources necessary to address the complexities of adapting criminal statutes to cyberspace. Literature reviewed in this study suggests that a coordinated, public-private partnership to produce a model approach can help reduce potential dangers arising from the inadvertent creation of cybercrime havens.

It is against this backdrop that the study seeks to develop a digital forensic readiness model (DFRM) using a coordinated, multidisciplinary approach, involving both the public and private sectors, thus enabling organisations to reduce potential dangers arising from the inadvertent destruction and negating of evidentiary data which, in turn, results in the non-prosecution of digital crimes.

The thesis makes use of 10 hypotheses to address the five research objectives, which are aimed at investigating the problem statement. This study constitutes qualitative research and adopts the post-modernist approach.

The study begins by investigating each of the 10 hypotheses, utilising a systematic literature review and interviews, followed by a triangulation of findings in order to identify and explore common themes and strengthen grounded theory results. The output from the latter process is used as a theoretical foundation towards the development of a DFRM model which is then validated and verified against actual case law.

Findings show that a multidisciplinary approach to digital forensic readiness can aid in preserving the integrity of evidentiary data within an organisation. The study identifies three key domains and their critical components. The research then demonstrates how the interdependencies between the domains and their respective components can enable organisations to identify and manage vulnerabilities which may contribute to the inadvertent destruction and negating of evidentiary data. The Multidisciplinary Digital Forensic Readiness Model (M-DiFoRe) provides a proactive approach to creating and improving organisational digital forensic readiness.

This study contributes to the greater body of knowledge in digital forensics in that it reduces

complexities associated with achieving digital forensic readiness and streamlines the handling of digital evidence within an organisation.

**Keywords:** digital forensics; forensic readiness; computer forensics; planning; investigation; risk management, evidence, cybercrime, multidisciplinary approach, triangulation, grounded theory, systematic literature review, qualitative research.

## DECLARATION

---

Student number: 4183-801-7

Study unit: DIS8524

I declare that DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING is my own work and that all the sources that I have used, or quoted, have been indicated and acknowledged by means of complete references.

I further declare that I have not previously submitted this work, or part of it, for examination at UNISA for another qualification, or at any other higher education institution.



Mr A Pooe (4183-801-7)  
School of Computing (Student)  
UNISA  
Pretoria

2011-04-20

### **Permission to conduct PhD:IS research project**

**Ref:016/AP/2011**

The request for ethical approval for your PhD(IS) research project entitled "Developing a multi-disciplinary digital forensic model for South African law enforcement: A mixed method study" refers.

The College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (CREC) has considered the relevant parts of the studies relating to the abovementioned research project and research methodology and is pleased to inform you that ethical clearance is granted for your study as set out in your proposal and application for ethical clearance.

Therefore, involved parties may also consider ethics approval as granted. However, the permission granted must not be misconstrued as constituting an instruction from the CSET Executive or the CSET CREC that sampled interviewees (if applicable) are compelled to take part in the research project. All interviewees retain their individual right to decide whether to participate or not.

We trust that the research will be undertaken in a manner that is respectful of the rights and integrity of those who volunteer to participate, as stipulated in the UNISA Research Ethics policy. The policy can be found at the following URL:

[http://cm.unisa.ac.za/contents/departments/res\\_policies/docs/ResearchEthicsPolicy\\_apprvCounc\\_21Sept07.pdf](http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf)

Please note that if you subsequently do a follow-up study that requires the use of a different research instrument, you will have to submit an addendum to this application, explaining the purpose of the follow-up study and attach the new instrument along with a comprehensive information document and consent form.

Yours sincerely

A handwritten signature in black ink, appearing to read "HH Lotriet".

**Prof HH Lotriet**

Acting Chair: School of Computing Ethics Sub-Committee



University of South Africa  
College of Science, Engineering and Technology  
Preller Street, Muckleneuk Ridge, City of Tshwane  
PO Box 392 UNISA 0003 South Africa  
Telephone + 27 12 429 6122 Facsimile + 27 12 429 6848  
[www.unisa.ac.za/cset](http://www.unisa.ac.za/cset)

## ACKNOWLEDGEMENTS

---

I wish to thank the following people, and the institutions which they represent, for their support during the course of my PhD studies:

- i. Prof. Lessing Labuschagne, my supervisor, for his strong leadership skills and passion for the research process.
- ii. Riana Zaayman, for the professional manner in which she always assisted with setting up meetings between Prof. Labuschagne and myself, and assisting with some administrative aspects of my research.
- iii. All participants who volunteered their time to assist me with interviews, consultations, editing and examining my thesis.
- iv. Finally, to my wife (Sonto Poee) and son (Lukhanya Poee), for their love and encouragement.

## TABLE OF CONTENTS

---

ABSTRACT.....	II
DECLARATION.....	IV
ETHICS CLEARANCE.....	V
ACKNOWLEDGEMENTS .....	VI
LIST OF FIGURES.....	X
LIST OF TABLES .....	XI
<b>1. CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
1.1 INTRODUCTION .....	1
1.2 MOTIVATION FOR THIS RESEARCH .....	2
1.3 PROBLEM STATEMENT .....	4
1.4 THE FIVE RESEARCH OBJECTIVES .....	4
1.5 THE 10 HYPOTHESES FOR INVESTIGATION.....	6
1.6 PURPOSE STATEMENT .....	7
1.7 ETHICAL CONSIDERATIONS .....	7
1.8 AN OVERVIEW OF THE LAYOUT OF THIS THESIS .....	9
1.9 CONCLUSION .....	12
<b>2. CHAPTER 2: SYSTEMATIC LITERATURE REVIEW .....</b>	<b>13</b>
2.1 INTRODUCTION .....	13
2.2 THE SYSTEMATIC LITERATURE REVIEW PROTOCOL .....	14
2.2.1 <i>Step 1: Define and refine a topic.....</i>	<i>14</i>
2.2.2 <i>Step 2: Design a search.....</i>	<i>15</i>
2.2.3 <i>Step 3: Locate the research literature .....</i>	<i>16</i>
2.2.4 <i>Step 4: Evaluate the results .....</i>	<i>17</i>
2.2.5 <i>Step 5: Write the review.....</i>	<i>18</i>
2.3 AN EVOLUTIONARY PRACTICE .....	22
2.3.1 <i>Components of the definition.....</i>	<i>24</i>
2.3.2 <i>Gaps in the definitions.....</i>	<i>24</i>
2.3.3 <i>Propositioned definition .....</i>	<i>25</i>
2.4 FINDINGS.....	25
2.4.1 <i>Hypothesis 1 .....</i>	<i>25</i>
2.4.2 <i>Hypothesis 2 .....</i>	<i>29</i>
2.4.3 <i>Hypothesis 3 .....</i>	<i>32</i>
2.4.4 <i>Hypothesis 4 .....</i>	<i>36</i>
2.4.5 <i>Hypothesis 5 .....</i>	<i>37</i>
2.5 CONCLUSION .....	41
<b>3. CHAPTER 3: RESEARCH DESIGN.....</b>	<b>43</b>
3.1 INTRODUCTION .....	43
3.2 THE RESEARCH DESIGN .....	43
3.2.1 <i>Ontology.....</i>	<i>44</i>
3.2.2 <i>Epistemology.....</i>	<i>45</i>
3.2.3 <i>Paradigm.....</i>	<i>45</i>
3.2.4 <i>Methodology.....</i>	<i>49</i>
3.2.5 <i>Research Method.....</i>	<i>50</i>
3.2.6 <i>Data Gathering Method .....</i>	<i>50</i>
3.2.7 <i>Analysing Method .....</i>	<i>51</i>

3.3	CONCLUSION .....	51
<b>4.</b>	<b>CHAPTER 4: DATA GATHERING AND ANALYSIS .....</b>	<b>53</b>
4.1	INTRODUCTION .....	53
4.2	DATA GATHERING METHOD.....	54
4.2.1	<i>Choice of Interview Types.....</i>	<i>54</i>
4.2.2	<i>The Interview Instrument.....</i>	<i>55</i>
4.2.3	<i>The Interviewees.....</i>	<i>55</i>
4.2.4	<i>Ethical Considerations.....</i>	<i>56</i>
4.3	ANALYSING METHOD .....	57
4.3.1	<i>The Data Analysis Tool.....</i>	<i>57</i>
4.3.2	<i>The Data Analysis Process.....</i>	<i>58</i>
4.4	FINDINGS .....	60
4.4.1	<i>Interviewee Profiles.....</i>	<i>60</i>
4.4.2	<i>Interview Responses.....</i>	<i>61</i>
4.4.3	<i>Hypothesis 6.....</i>	<i>62</i>
4.4.4	<i>Hypothesis 7.....</i>	<i>63</i>
4.4.5	<i>Hypothesis 8.....</i>	<i>63</i>
4.4.6	<i>Hypothesis 9.....</i>	<i>64</i>
4.4.7	<i>Hypothesis 10.....</i>	<i>64</i>
4.5	INTERPRETATION OF FINDINGS .....	65
4.5.1	<i>Corporate Environment.....</i>	<i>67</i>
4.5.2	<i>Industry Environment.....</i>	<i>68</i>
4.5.3	<i>Legislative Environment.....</i>	<i>69</i>
4.5.4	<i>Development of final themes from code families and networks.....</i>	<i>70</i>
4.6	TRIANGULATION OF FINDINGS .....	74
4.7	CONCLUSION .....	76
<b>5.</b>	<b>CHAPTER 5: FOUNDATIONAL PRINCIPLES TOWARDS MODEL DEVELOPMENT .....</b>	<b>78</b>
5.1	INTRODUCTION .....	78
5.2	OVERVIEW OF THE COMPONENTS OF THE PROPOSED MODEL .....	78
5.2.1	<i>The Corporate Environment (CE).....</i>	<i>78</i>
5.2.2	<i>The Industry Environment (IE).....</i>	<i>82</i>
5.2.3	<i>The Legislative Environment (LE).....</i>	<i>87</i>
5.2.4	<i>The Multidimensional Effect.....</i>	<i>92</i>
5.3	THE CONCEPTUAL MODELLING PROCESS .....	94
5.3.1	<i>Procedural Guidelines.....</i>	<i>94</i>
5.3.2	<i>Applied Modelling Process.....</i>	<i>95</i>
5.4	CONCLUSION .....	97
<b>6.</b>	<b>CHAPTER 6: REALISATION OF THE CONCEPTUAL MODEL.....</b>	<b>98</b>
6.1	INTRODUCTION .....	98
6.2	MODEL DEVELOPMENT PROTOCOL.....	99
6.2.1	<i>Scoping and Database Section.....</i>	<i>99</i>
6.2.2	<i>Selected Case Law.....</i>	<i>100</i>
6.3	FINDINGS.....	100
6.3.1	<i>Case Law Synopses.....</i>	<i>100</i>
6.3.2	<i>Process for Data Coding.....</i>	<i>102</i>
6.3.3	<i>Mapping of Code Families.....</i>	<i>104</i>
6.4	A MULTIDISCIPLINARY CONCEPTUAL DIGITAL FORENSIC READINESS MODEL.....	113
6.4.1	<i>The Analogy.....</i>	<i>114</i>
6.4.2	<i>Model Functionality.....</i>	<i>114</i>
6.5	M-DiFoRE MODEL KEY DIFFERENTIATORS.....	122
6.5.1	<i>Systematic Classification of Critical Components.....</i>	<i>122</i>
6.5.2	<i>Strategic Codification of Component Interdependencies.....</i>	<i>122</i>



6.5.3	<i>Cross-Functional Approach with Multiple Starting Points.....</i>	123
6.5.4	<i>Non-Context Specific (Universal) Application.....</i>	123
6.6	CONCLUSION .....	124
<b>7.</b>	<b>CHAPTER 7: MODEL VALIDATION APPROACH.....</b>	<b>126</b>
7.1	INTRODUCTION .....	126
7.2	VALIDATION PROTOCOL.....	127
7.3	VALIDATION OF MODEL .....	127
7.3.1	<i>Activity 1 - Case Law Synopsis: Defamation and Unlawful Competition.....</i>	127
7.3.2	<i>Activity 2 - Self Assessment.....</i>	128
7.3.3	<i>Activity 3 - Qualitative Analysis.....</i>	134
7.3.4	<i>Activity 4 - Results Comparison.....</i>	144
7.3.5	<i>Activity 5 – (Step 4) Remedial Action.....</i>	147
7.4	CONCLUSION .....	151
<b>8.</b>	<b>CHAPTER 8: CONCLUSION.....</b>	<b>153</b>
8.1	INTRODUCTION .....	153
8.2	CHAPTER SUMMARY.....	153
8.2.1	<i>Chapter 1: Introduction .....</i>	154
8.2.2	<i>Chapter 2: Systematic Literature Review.....</i>	154
8.2.3	<i>Chapter 3: Research Design.....</i>	155
8.2.4	<i>Chapter 4: Data Gathering And Analysis.....</i>	155
8.2.5	<i>Chapter 5: Foundational Principles Towards Model Development .....</i>	156
8.2.6	<i>Chapter 6: Realisation of the Conceptual Model.....</i>	157
8.2.7	<i>Chapter 7: Model Validation Approach.....</i>	157
8.3	REVISITING THE PROBLEM STATEMENT .....	158
8.4	REVISITING THE PURPOSE STATEMENT .....	159
8.5	RESEARCH CONTRIBUTION TO BODY OF KNOWLEDGE .....	160
8.6	RESEARCH LIMITATIONS .....	160
8.7	FUTURE RESEARCH OPPORTUNITIES.....	162
8.8	THE RESEARCH VALUE .....	162
8.9	SELF-REFLECTION .....	163
	<b>REFERENCES .....</b>	<b>165</b>
	<b>APPENDIX 1: PAPER PRESENTED AT ISSA 2012, SOUTH AFRICA .....</b>	<b>184</b>
	<b>APPENDIX 2: PAPER PRESENTED AT IFIP 2014, UNITED STATES OF AMERICA.....</b>	<b>192</b>
	<b>APPENDIX 3: INTERVIEW INSTRUMENT .....</b>	<b>209</b>
	<b>APPENDIX 4: INTERVIEW CONSENT LETTER.....</b>	<b>212</b>
	<b>APPENDIX 5: CASE STUDY 1: ATLAS.TI CODING SUMMARY REPORT .....</b>	<b>216</b>
	<b>APPENDIX 6: CASE STUDY 2: ATLAS.TI CODING SUMMARY REPORT .....</b>	<b>229</b>
	<b>APPENDIX 7: CASE STUDY 3: ATLAS.TI CODING SUMMARY REPORT .....</b>	<b>236</b>
	<b>APPENDIX 8: CASE STUDY 4: ATLAS.TI CODING SUMMARY REPORT .....</b>	<b>241</b>
	<b>APPENDIX 9: COMPLETED SELF-ASSESSMENT .....</b>	<b>246</b>

## LIST OF FIGURES

---

Figure 1: SWGDE Data integrity within computer forensics (SWGDE, 2006). .....	27
Figure 2: The paradigm and methodological choices in scientific research (adapted). .....	44
Figure 3: Data analysis process summary using Atlas.ti .....	60
Figure 4: Summary of network maps formed from analysis of interview data. ....	66
Figure 7: Interdependencies between IE2 and LE2 .....	106
Figure 8: Interdependencies between IE6 and LE5. ....	107
Figure 9: Interdependencies between IE8 and LE4. ....	107
Figure 10: Interdependencies between CE4, LE3 and IE2. ....	108
Figure 11: Interdependencies between IE8, CE1 and LE1. ....	109
Figure 12: Interdependencies between CE2, IE8 and LE1. ....	110
Figure 13: Interdependencies between CE4, IE8 and LE2. ....	110
Figure 14: Interdependencies between IE8, CE3 and LE2. ....	111
Figure 15: Interdependencies between CE5, IE1 and LE2. ....	112
Figure 16: Interdependencies between LE3 and the industry environment as represented by components IE1 to IE9. ....	113
Figure 17: The Multidisciplinary Digital Forensic Model (M-DiFoRe Model). ....	116
Figure 19: Analysis of the Evidence Collection system. ....	136
Figure 20: Analysis of the Justice System Implementation system. ....	137
Figure 21: Analysis of the e-Crime Prosecution system. ....	137
Figure 22: Analysis of the Evidence Handling system. ....	138
Figure 23: Analysis of the Standards Localisation system. ....	139
Figure 24: Analysis of the Policy Alignment system. ....	140
Figure 25: Analysis of the Witness Preparation system. ....	141
Figure 26: Analysis of the Procedural Implementation system. ....	141
Figure 27: Analysis of the Evidence Preservation system. ....	142
Figure 28: Analysis of the Methodology Evaluation system. ....	144

## LIST OF TABLES

---

Table 1: Relationship between literature themes and hypotheses. ....	5
Table 2: Overview of the layout of this thesis. ....	11
Table 3: Reference materials used to identify articles for inclusion.....	17
Table 4: The application of Cohen's Kappa (K) to this study.....	18
Table 5: Digital Forensic Models reviewed.....	21
Table 6: Elements of the digital forensics definition. ....	24
Table 7: ACFE SA reference resources for the creation of a common digital forensic standard in South Africa. ....	31
Table 8: A sample of modern anti-forensic tools and their functionality.....	35
Table 9: Summary of interviewee profiles.....	61
Table 10: Summary of the relationship between hypotheses 6 to 10, interview questions and related research objectives. ....	62
Table 11: Code themes developed from analysis of interview data. ....	70
Table 12: Corporate Environment - transition from preliminary to final codes.....	71
Table 13: Industry Environment - transition from preliminary to final codes.....	72
Table 14: Industry Environment - transition from preliminary to final codes.....	73
Table 15: Final code themes developed from analysis of the interview data and literature relating to hypothesis 6 to 10.....	73
Table 16: Summary of results from Chapters 2 and 4. ....	75
Table 17: Characterisation of components. ....	92
Table 18: Link and arrow types used to investigate relationships between components. ....	103
Table 19: Self-Assessment template for using the M-DiFoRe model to identify vulnerable systems.....	121
Table 20 Step 1: Self-Assessment Results.....	129
Table 22 Step 3: Self-Assessment Results.....	133
Table 23 Comparison of self-assessment results to qualitative analysis. ....	147
Table 24 Recommended remedial action on vulnerable systems .....	149

## **1. Chapter 1: Introduction**

---

### **1.1 Introduction**

The integration of information and communication technologies (ICT) into daily life, be it commercial, educational or governmental, has not only improved the productivity but also the efficiency of these entities. In the same manner, criminals have identified ways in which traditional crimes can be committed using computing power and accessibility to information. In these crimes, technology is primarily used either as a tool to commit or a repository of evidence related to a crime (Kizza, 2007; Noblett et al., 2000).

Noblett et al. (2000) found that the reality associated with digital forensic science is the lack of a consistent *methodology*. The evolution of digital forensics has proceeded from ad hoc tools and techniques, rather than from the scientific community, from which many of the other traditional forensic sciences have originated (Reith et al., 2002). This creates a challenge when it comes to ensuring that electronic evidence is discovered using scientific and proven methods. It is this *challenge* that has elevated cybercrime to the crime of choice since the chances of being prosecuted are much slimmer than in traditional criminal law matters such as fraud, theft and corruption (Curtis, 2012; Interpol, 2013).

In addition, much has been done to define the key steps involved in the digital forensic process. Reith et al. (2002) highlight that tools, such as the Coroner's Toolkit, are based on gaps that existed in methodologies related to Unix based systems. Other noteworthy contributors to the digital forensic process include the Department of Justice (National Institute of Justice, 2001) and the Digital Forensics Research Workshop (Digital Forensic Research Workshop, 2016). The result of all the preliminary work has been the development of at least three distinct digital forensic models: The Abstract Digital Forensics Model (Reith et al., 2002), The Integrated Digital Investigation Model (Carrier et al., 2003) and The Enhanced Integrated Digital Investigation Model (Baryamureeba et al., 2004).

Much work has been done to standardise practices relating to the process of digital forensic investigations. In its simplest sense, a standard is an agreed-upon way of doing something (Spivak et al., 2001) and as such it forms a cornerstone of the modern information economy (Greenstein et al., 2007). *Standards* are a means of creating order as they denote a uniform set

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

of measures, agreements and conditions (Spivak et al., 2001; Grindley, 1995). In other words, standards act as a form of regulation. Their usage in the industry may be voluntary, or in some cases, mandatory. Many standards are used voluntarily, but in time they may become adopted, or referenced, into mandatory regulations (Spivak et al., 2001).

Over the past decade, well-understood procedures and methodologies have evolved within the domain of digital evidence collection (Kenneally et al., 2005; Cooper et al., 2010). For this reason, this study ventures into establishing the effect that a localised digital forensic readiness model (DFRM) could have on the admissibility of electronic evidence in a court of law. As Curtis (2012) explains, ICT related crimes go beyond the use of a computer alone but include other forms of technologically advanced devices as well. For the purposes of this study, the term *digital* will be used as an all-encompassing term to refer to electronic devices that may be used for the purpose of committing a crime.

This chapter describes the motivation for the thesis, presents a preliminary literature review to contextualise the problem statement and the related research objectives and details how a set of hypotheses was used to investigate each of the said research objectives (Table 1). The aforementioned is conducted by following a specific research process and in accordance with certain philosophical choices (Figure 1). Finally, the chapter presents a diagram which outlines the chapter layout of this thesis (Table 2).

### **1.2 Motivation for this research**

The motivating factor for this research was derived from the researcher's observations regarding the *challenges* which organisations face when they attempt to prosecute digital crimes. McConnel International (2000) and Obuh (2011) found that, at a time when greater emphasis is being placed on issues like violent crime reduction and community-based policing, the detection and investigation of technology-related offenses remain an elusive goal. Simply stated, findings suggest that digital crime is not a priority for police departments around the world.

Walsh et al. (2013) found that for digital cases reported to *authorities*, the prosecution thereof raises many issues regarding the consistency of standards, *problems* with the statutory framework and the suitability of the punishments being sought. Walsh et al. (2013) further argued that charges against the defendant/s were ultimately often dismissed due to *problems*

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

with the police investigation or forensic examination.

In addition, Walsh et al. (2013) noted supplementary *contributing difficulties* which included: the lack of timeliness of the computer forensics examination, the lack of equipment or training of officers and issues with search warrants. Goodman (1997) found that the business community generally believes that police officers cannot handle computer-related crimes and security problems because they think that the police do not grasp the issues. Additionally, corporate managers believe that police agencies are ineffective, and their involvement counter-productive, in prosecuting or restricting computer crime.

McConnell International (2000) and Obuh (2011) state that the prevalence of computer crimes will continue to increase because it is easy to learn how to commit them; they require few resources relative to the potential damage they can cause; they can be committed in a jurisdiction in which the perpetrator is not physically present and they are often not explicitly illegal.

This situation is further exasperated by weak penalties which, in turn, provide limited deterrence to crimes that can have large-scale economic and social effects (Goodman, 1997; Obuh, 2011). In addition to weak penalties, Obuh (2011) found that mechanisms of cooperation across national borders toward solving and prosecuting crimes are not only complex, but slow.

Gershowitz (2011) found that, in addition to the challenges already discussed, the prosecutorial process favours cyber criminals as it is difficult to convince a typically overburdened prosecutorial office to commit resources to see the matter through to conviction. Most prosecutors with limited *resources* devote their efforts to addressing those crimes perceived as posing the greatest threat.

A study reported that, in South Africa, businesses generally *lack* the ability to detect, track, prove and prosecute cases of cyber-based fraud (ITWeb, 2013). Furthermore, investigations and prosecutions are hampered by a lack of forensic readiness on the part of the companies affected. ITWeb (2013) reports that “in South Africa, it is estimated that less than 6% of all criminal cases are successfully prosecuted. With cyber-based crimes, the conviction rate could be even lower due to its technical nature.”

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Finally, McConnell International (2000, p. 8) established that most countries, particularly those in the developing world, “recognise the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for e-commerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyberspace. A coordinated, public-private partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cybercrime havens.”

It is against this backdrop that the study explores the development of a multidisciplinary digital forensic readiness model for use in developing economies, utilising South Africa as a case study.

The next section will discuss the problem statement.

### **1.3 Problem Statement**

Derived from the preliminary literature review, as presented above, the problem statement for this study can be formulated in the following way:

The organisational risk of inadvertently destroying and negating evidentiary data, due to the complexity and multidisciplinary nature of digital crimes, necessitates the development of a digital forensic readiness model using a coordinated, multidisciplinary approach involving both public and private sectors. Current models are context, technology and/or business process specific, and lack the multidisciplinary approach which seeks to investigate inter-discipline interactions.

In order to investigate potential solutions to the above problem statement, a set of research objectives was developed. These are discussed next.

### **1.4 The Five Research Objectives**

The following research objectives were derived from prominent literature themes that stem from the preliminary literature review conducted as part of this research proposal (see italicised Sections 1.1 and 1.2 for keywords [literature themes] which led to the development of the research objectives).

- i. Research Objective 1 (RO1): To identify common factors associated with both the

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

*technical and legal challenges* faced in the prosecution of digital crimes.

- ii. Research Objective 2 (RO2): To establish whether organisations in the same legal jurisdiction have, and make use of, a standard *digital forensics methodology*.
- iii. Research Objective 3 (RO3): To determine the extent to which *advances* in digital forensics are meeting the demands of the changing legal and technical landscape.
- iv. Research Objective 4 (RO4): To investigate critical factors preventing *human resources* directly involved in the investigation and prosecution of digital crimes from functioning effectively.
- v. Research Objective 5 (RO5): To determine whether organisations are taking the necessary steps to *proactively manage* the rising scourge of digital crimes.

In addition, a series of 10 hypotheses was used to explore the problem statement and associated research objectives. These hypotheses are distributed equally and investigated in Chapters 2 and 4, respectively. For purposes of triangulation, more than one method of data collection on the same phenomenon is used (Craig, 2009). This process facilitates the validation of data through cross verification from two, or more, sources as a means to increase confidence in the results (Yin, 2011).

Each hypothesis is theoretically explored using a literature survey, as presented in Chapter 2. In Chapter 4 field interviews with industry experts are presented as the second means of exploring each hypothesis.

See Table 1 for a summary of the relationship between the literature themes, research objectives (RO) and hypotheses (H).

<b>Literature Themes</b>	<b>Research Objectives</b>	<b>Chapter 2 (Systematic Literature Review)</b>	<b>Chapter 4 (Data Gathering and Analysis)</b>
Technical and Legal Challenges	RO1	H <sub>1</sub>	H <sub>6</sub>
Digital Forensic Methodology	RO2	H <sub>2</sub>	H <sub>7</sub>
Digital Forensic Advances	RO3	H <sub>3</sub>	H <sub>8</sub>
Human Resource Management	RO4	H <sub>4</sub>	H <sub>9</sub>
Digital Crime Preparedness	RO5	H <sub>5</sub>	H <sub>10</sub>



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Table 1: Relationship between literature themes and hypotheses.

The next section discusses the 10 hypotheses investigated in this thesis.

### **1.5 The 10 Hypotheses for Investigation**

This section presents the 10 hypotheses and shows their distribution across Chapters 2 and 4.

Chapter 2 presents the following five hypotheses, which were tested by means of a Systematic Literature Survey (Sobh, 2010):

- i. Hypothesis 1 (H1): Electronic evidence gathered during a digital forensic investigation does not provide sufficient assurance of non-manipulation to the courts.
- ii. Hypothesis 2 (H2): There is a lack of standardisation of the criteria against which electronic evidence is validated as no consistent digital forensic methodology exists.
- iii. Hypothesis 3 (H3): Forensic technology for gathering digital evidence is increasingly lagging behind the advances being made in anti-forensic tools and the rapid changes in storage technology.
- iv. Hypothesis 4 (H4): Individuals involved in the digital forensic investigation and prosecution process are not sufficiently trained and/or educated.
- v. Hypothesis 5 (H5): An organisation responding to a digital crime, without an incident response plan, may take actions that compromise the admissibility of evidence to a court of law.

Chapter 4 uses interviews (Teddlie et al., 2009; Kvale et al., 2009) to test the following 5 hypotheses:

- i. Hypothesis 6 (H6): As a result of the presence of the electronic laws in South Africa, the prosecution of digital crimes faces no limitations.
- ii. Hypothesis 7 (H7): South Africa has a standardised digital forensic model and process which is used by authorities to investigate and prosecute digital crimes.
- iii. Hypothesis 8 (H8): The Electronic Communications and Transactions (ECT) Act of South Africa adequately positions the acceptable use of, and extent to which, electronic evidence can be used in a civil or criminal proceeding.
- iv. Hypothesis 9 (H9): Those individuals involved in the prosecution of digital crimes are knowledgeable, adequately trained and professionally certified.
- v. Hypothesis 10 (H10): South African organisations do not need to concern themselves

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

with digital forensic readiness, as digital crimes are not commonplace.

The next section discusses the purpose statement and the adopted research design.

### **1.6 Purpose Statement**

The purpose of this study is to develop and explain how a model based, multidisciplinary approach to digital forensic readiness can aid in preserving the integrity of evidentiary data within an organisation.

According to McConnell International (2000), such a model and approach may help eliminate the potential danger posed by the inadvertent destruction and negating of evidentiary data.

For purposes of this research, the scope is limited to the South African legal context.

### **1.7 Ethical Considerations**

This research was conducted in strict adherence to the University of South Africa's Policy on Research Ethics (UNISA, 2007). At the time of thesis submission, a revised version of said policy existed, the requirements of which were also taken into consideration to ensure strict compliance. Compliance was achieved in all aspects, particularly regarding the following requirements relating to general ethics principles:

- i. **Essentiality and relevance:** the requirement is to consider the scarcity of resources in South Africa and to demonstrate that the research is in pursuit of knowledge and public good. In doing so, a rigorous review of South African case studies was analysed, in conjunction with the systematic literature review findings, to understand the underlying issues relating to the topic under investigation. The research topic also serves the public good in that it addresses a pertinent and relevant issue.
- ii. **Maximisation of public interest and social justice:** the requirement is to conduct research for the benefit of society, with the motive of maximising public interest and social justice by sharing the research findings with the public. This thesis specifically addresses social challenges, as they relate to the prosecution of digital crimes. Articles on key findings of this research were made public through publications in research journals.
- iii. **Competence, ability and commitment to research:** the requirement is for the researcher

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

to be both personally, and professionally, qualified for the research which he/she undertakes. In this instance, as at the time of this research, the researcher has over ten years of experience as a digital forensic practitioner, and holds relevant international certifications and qualifications in the field.

- iv. Respect for and protection of the rights and interests of participants and institutions: the requirement is to respect and protect the dignity, privacy and confidentiality of participants and institutions alike. To achieve this, the thesis maintains the anonymity of both the participants and their institutions. All personally identifiable data is encrypted and stored in a secure location.
- v. Informed and non-coerced consent: the requirement is that individuals freely participate, based on informed consent and for a specific purpose. Participants in this study were informed of their rights and formal permission to participate required in a written letter. Their acceptance was in the form of counter signing the said letter, which was also kept safe, in encrypted format as it contains personally identifiable data.
- vi. Respect for cultural differences: the suggestion is for research to be undertaken *with* the members of an identified community, or communities, rather than merely *about* such a community, or communities. No cultural challenges were faced during the selection of said participants.
- vii. Justice, fairness and objectivity: the requirement is for the selection criteria of research participants to be fair and scientific. The participants in this research were experts in the industry, who had met a strict criterion, as further detailed in Chapter 3.
- viii. Integrity, transparency and accountability: the guideline is that researchers should be honest about their own limitations, competence, belief systems, values and needs. To ensure adherence to these principles, this thesis details the research approach followed (see section 1.7 of Chapter 1), and strictly applies the scientific process associated with the interpretive paradigm. The researcher's personal opinions are detailed in Chapter 8, in the form of reflections on the research undertaken.
- ix. Risk minimisation: the requirement is that actual benefits to be derived by the participants, or society, clearly outweigh any possible risks, and that participants are subjected only to those risks that are clearly necessary for the conduct of the research. This thesis protects the anonymity of the participants and their institutions, thereby avoiding any possible backlash resulting from exposure.
- x. Non-exploitation: the requirement is for there to be no exploitation of research participants, researchers (including students and junior members), communities, institutions or vulnerable people. All participants of this study were treated with respect

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

and in a professional manner. Careful preparation was conducted, prior to meeting with participants, to demonstrate that their time and efforts were valued.

All other sections of the Ethics Policy were carefully read and considered.

A copy of the signed ethics clearance is attached to this thesis. The next section presents an overview of the layout of the thesis.

### **1.8 An Overview of the Layout of this Thesis**

As per Table 2, this study comprises eight chapters and a conclusion.

Chapter 1: This chapter presents the introduction. It details the problem statement and the five research objectives, as derived from the literature survey conducted. This work is presented in Chapter 1, as part of the research proposal.

Chapter 2: This chapter discusses the first set of five hypotheses, each linked to a research objective which, in turn, contributes to achieving the requirements of the problem statement. A systematic literature review was used as a data gathering method and to test each hypothesis. This chapter demonstrates *how* the relativist ontology, as discussed in Chapter 3, was applied to analyse the primary research data. A new digital forensic conceptual model is presented.

A research paper was published at the conclusion of this chapter. See Appendix 1 for a copy of this research article which proposes the conceptual model developed as part of the output from Chapter 2.

Chapter 3: Outlines the methodology, ontology and epistemology adopted in this research, and provides justification for the same.

Chapter 4: This chapter presents hypotheses 6 to 10, and comprises the main experiment section of this research. Interviews were the data gathering method used to test each of the hypothesis presented in this chapter, as part of the human experiment to confirm results from Chapter 2 (systematic literature survey). This chapter demonstrates the application of the interpretivist paradigm in order to facilitate the analysis and interpretation of interview data collected. Finally, this chapter discusses the triangulation of findings from chapters 2 and 4, in order to identify and explore common themes and strengthen grounded theory results. The output from

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

the latter process is used as a theoretical foundation towards the development of the proposed model which is then validated and verified against actual case law.

A research paper was published at the conclusion of this chapter. See Appendix 2 for a copy of the research article describing the proposed high-level multidisciplinary model.

Chapter 5: Presents a discussion regarding the significance of the three key environments which contextualise digital forensic readiness and each of their respective components, and uses a critical literature review to support the assertions made. This chapter forms the foundation upon which the proposed multidisciplinary model was developed.

Chapter 6: This chapter takes the cumulative findings from the previous chapters and validates them against three case studies, leading to the creation of the M-DiFoRe model. Principles of relativism, as discussed in Chapter 1 (see section 1.7), are applied as the main ontological position taken in the validation and verification of the model, as presented in Chapters 6 and 7, respectively.

Chapter 7: This chapter contains the details of how the M-DiFoRe model was verified. This verification process served as a basis to assess whether the model meets the requirements, as stipulated in the problem statement.

Chapter 8: This is the concluding chapter, which outlines a summary of the key findings of this study is presented, along with the research value and opportunities for further research.

Throughout the thesis, a simplistic approach was purposefully adopted in explaining and defining certain terms. This was done to make the research more accessible to a broader audience.

DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

Problem Statement	Chapter 1	Chapter 2	Chapter 4	Chapter 5	Chapter 6	Chapter 7	
<p>The organisational risk of inadvertently destroying and negating evidentiary data due to the complexity and multidisciplinary nature of digital crimes, necessitates the development of a digital forensic readiness model using a coordinated, multidisciplinary approach involving both the public and private sectors. Current models are context, technology and/or business process specific, and lack the multidisciplinary approach that seeks to investigate inter-discipline interactions.</p>	1. RO1	H1	H6 (INT Q6, Q10, Q15)	<p><i>Part 1: Conceptual Model development</i></p>	<p><i>Part 2: Model development using a coordinated and multidisciplinary approach</i></p>	<p><i>Model assessment</i></p>	
	2. RO2	H2	H7 (INT Q5, Q7, Q11)				
	3. RO3	H3	H8 (INT Q8, Q9, Q4)				
	4. RO4	H4	H9 (INT Q12, Q13, 14)				
	5. RO5	H5	H10 (INT Q1, Q2, Q3)				
	<p><i>Chapter 3 - Approach: Postmodernism</i></p>						
	<p><i>Chapter 3 - Ontology: Relativism</i></p>						
	<p><i>Chapter 3 - Epistemology: Interpretivism</i></p>						
	<p><i>Chapter 3 - Paradigm: Interpretivist</i></p>						
	<p><i>Chapter 3 - Methodology: Grounded Theory</i></p>						
	<i>Introduction</i>	<i>Systematic Literature Review</i>	<i>Data Gathering and Analysis</i>	<i>Foundational Principles Towards Model Development</i>	<i>Realisation of the Conceptual Model</i>	<i>Model Validation Approach</i>	

[RO<sub>n</sub> – Research Objective; H<sub>n</sub> – Hypothesis; INT Q<sub>n</sub> – Interview Question]

Table 2: Overview of the layout of this thesis.

# DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

## 1.9 Conclusion

This chapter presented an introduction to this research, and outlined the motivation for this research, problem statement, research objectives, and the purpose statement.

The research objectives were divided equally (into sets of five) and spread across Chapters 2, and 5, for further investigation and testing. Each of the hypotheses was linked to a research objective and collectively they formed the basis for investigating the problem statement.

Finally, this chapter concludes with a presentation on the layout of the thesis and briefly discusses the contents of the eight chapters.

Chapter 2, which contains a systematic literature survey, is presented next.

## **2. Chapter 2: Systematic Literature Review**

---

### **2.1 Introduction**

The previous chapter comprised the research proposal and presented the layout of this thesis.

The aim of this chapter is to establish whether challenges experienced with the digital forensic process have any empirical grounding in literature. This is done by investigating hypotheses 1 to 5 and making use of a systematic literature survey, as a research method, in the investigation process. The hypotheses under investigation are:

- i. Hypothesis 1 (H1): Electronic evidence gathered during a digital forensic investigation does not provide sufficient assurance of non-manipulation to the courts.
- ii. Hypothesis 2 (H2): There is a lack of standardisation in the criteria against which electronic evidence is validated as no consistent digital forensic methodology exists.
- iii. Hypothesis 3 (H3): Forensic technology for gathering digital evidence is increasingly lagging behind the advances being made in anti-forensic tools and the rapid changes in storage technology.
- iv. Hypothesis 4 (H4): Individuals involved in the digital forensic investigation and prosecution process are not sufficiently trained and/or educated.
- v. Hypothesis 5 (H5): An organisation responding to a digital crime, without an incident response plan, may take actions that compromise the admissibility of evidence to a court of law.

The results from testing these hypotheses provided a theoretical foundation to understanding existing literature relating to the research objectives and also facilitated the extrapolation of common themes and patterns in literature which, in turn, guided the development of the digital forensic ready (DFR) conceptual model, as detailed in the published research paper attached herein as Appendix 1.

The chapter concludes with a discussion on the outcome of each hypothesis.



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **2.2 The Systematic Literature Review Protocol**

A systematic literature review is used to conduct the literature review. Unlike conventional literature reviews, a systematic review follows a predefined protocol. It is defined as a way to “identify, evaluate and interpret the available research that is relevant to an issue or discipline, or phenomenon of interest of a specific research domain” (Sobh, 2010, p. 99).

Systematic reviews require the researcher to systematically collect all the search on a given topic, select studies according to pre-determined quality criteria, abstract the same information from each included study, display the results in evidence tables and then interpret the results in light of the totality of the evidence (Lang, 2010).

Fox et al. (2007) summarised the steps for a systematic literature review as follows:

- i. Step 1: Define and refine a topic. A literature review starts with a clearly defined, well-focused research question and a plan. Keywords are used to aid the search for related research material for review.
- ii. Step 2: Design a search. It is important to decide on the type of literature review, its extent and the types, or forms, of literature to include (parameters).
- iii. Step 3: Locate the research literature. Locating the relevant literature will depend on the type of literature being sought.
- iv. Step 4: Evaluate the results and determine what to record. Located literature must be evaluated and recorded in a suitable way. If sources do not provide sufficient information, it is important to revisit the retrieval system and use a different approach. Whatever the method used, the search must be systematic and organised.
- v. Step 5: Write the review. A systematic literature review requires planning and good, clear writing.

This protocol is adopted with the aim of achieving a high level of scientific rigour, thus enhancing the reliability of the research output. The next section discusses the way in which these steps were applied in the thesis.

#### **2.2.1 Step 1: Define and refine a topic**

The research question governing this chapter is: do the challenges experienced with the digital forensic process have any empirical grounding in literature?

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

The following keywords were used:

- i. Digital forensics;
- ii. Computer forensics;
- iii. Forensic readiness;
- iv. Digital forensic methodology and
- v. Digital forensic process.

### 2.2.2 Step 2: Design a search

The scope of our research was limited to material available on the University of South Africa Online Library (UNISA, 2010a). This library is said to be one of the largest libraries in Africa, with information sources in excess of 1.5 million. The library also subscribes to an increasing number of electronic journals, which are available at all times to Unisa students (Ramalibana, 2005; UNISA, 2010a).

A detailed search of relevant databases was conducted. The relevance was determined by using the library's A - Z list of electronic resources (UNISA, 2010b). From this, databases containing the most relevant material were selected and analysed further in search of articles and other publications. The databases used were selected based on them being classified under the following categories:

- i. Multidisciplinary;
- ii. Computing;
- iii. Law;
- iv. Information Science and
- v. Engineering.

Furthermore, the databases used were those which contained the majority of search hit results. The search word used was *digital forensic*. This keyword was used as the basis of the search as it directly relates to the topic under investigation.

Only English written material (published 2002 – 2017) was reviewed. The reasons for this being that firstly, Unisa's online library is available in English and it is one of South Africa's most commonly spoken languages in business, politics and the media (Webb, 2002; South Africa, 2013).

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Secondly, there was no law on digital crimes in South Africa prior to the Electronic Communications and Transactions Act in 2002 (Government Gazette, 2002; Kabanda et al., 2010). Therefore, only articles written after promulgation of this law were taken into consideration.

The decision for reviewing only articles was based on the logic that articles usually flow from books, dissertation and theses. Therefore, by looking at articles, content from the latter is also covered. The next section discusses the methodology for the screening of articles for inclusion.

### **2.2.3 Step 3: Locate the research literature**

Table 3 shows the seven disciplines from which the included articles were obtained. This table also shows the database searched under each discipline. In order to ensure that the process of identifying articles for inclusion was comprehensive, the following methodology was followed:

- i. Open the UNISA online library link (UNISA 2010a);
- ii. Search for resources according to subject;
- iii. Select the subject/discipline topic;
- iv. Identify and select the relevant journal;
- v. Search entire journal collection for articles with keywords “digital forensics, computer forensics, forensic readiness, digital forensic methodology, digital forensic process”;
- vi. Read the abstract of the first 100 articles appearing on the results page;
- vii. Export only the full text of articles selected for inclusion, based on the relevance established from the abstract and
- viii. Detailed analysis of articles of inclusion.

The use of these eight steps ensured that every article, in each journal, found in every database of inclusion, was reviewed for relevance.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

#	Discipline	Database Name	Journal
1	Computing	Association of Computing Machinery ACM Digital Library	All
2	Engineering	ProQuest Technology Journals	All
3	Law	Oxford University Press Journals (current and archive)	All
4	Consumer Science	ScienceDirect	All
5	Library & Information Science	ScienceDirect	All
6	Police Practice	Criminal Justice Periodicals	All
7	Science and Technology	Scitopia	All

Table 3: Reference materials used to identify articles for inclusion.

#### 2.2.4 Step 4: Evaluate the results

Since this systematic literature review is aimed not only at publication purposes, but also for instrumental utilisation, an additional screening process was undertaken to increase the reliability of the results. The researcher and supervisor conducted the screening process on a subset of articles, independently of each other, and then met to compare results. In order to ensure that this process was scientific, the Cohen's Kappa (K) inter-rater was used for measuring reliability of this process. Inter-rater reliability is the degree of agreement between two observers who have independently observed and recorded behaviours at the same time (Gravetter et al., 2009; Mathews, 2010). The basic formula for Cohen's Kappa (K) is computed as illustrated below:

$$\begin{aligned} \text{Cohen's Kappa} &= \frac{PA (0.77) - PC (0.50)}{1 - PC (0.50)} \\ &= 0.54 \end{aligned}$$

Where *PA* is the observed percentage agreement and *PC* is the percentage agreement expected (Gravetter et al., 2009).

The goal in this study was to produce a *PA* value above 75% from the total reviewed articles. This was computed in the following way:

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

$$PA = \frac{\text{Articles which both Researcher and Supervisor agree on for inclusion}}{\text{Total number of articles reviewed}} > 75\%$$

The overall application of Cohen’s Kappa (K) inter-rater in the review of articles for inclusion is shown in Table 4.

		<b>Supervisor's Decisions</b>		
		Articles Included	Articles Excluded	
<b>Researcher's Decisions</b>	Articles Included	A	B	A + B
	Articles Excluded	C	D	C + D
		<b>A + C</b>	<b>B + D</b>	<b>A+B+C+D</b>

Table 4: The application of Cohen's Kappa (K) to this study.

As stated before, the goal was to produce a *PA* value above 75% from the total reviewed articles. This was done to ensure that all relevant articles were included for detailed review and to archive a kappa value above 0.50. The said kappa goal is generally considered to be satisfactory (Gravetter et al., 2009; Mathews, 2010).

Both authors met to calculate the inter-rate reliability by calculating a percentage agreement. This process was repeated until the percentage agreement exceeded 75%. Abstracts of 459 articles were reviewed, resulting in the identification of 130 relevant articles for possible inclusion. The review process was refined further and the result was an agreement on the final 100 articles for inclusion.

The next section discusses the articles reviewed and their relevance to this study.

### **2.2.5 Step 5: Write the review**

Since the advent of the Electronic Communications and Transactions Act of 2002 (Government Gazette, 2002), electronic evidence has increasingly been accepted in the modern South African courtroom. A paradigm shift from the traditional law of evidence had to take place in order to accommodate the unique complexities that digital evidence carries (Gershowitz, 2011, Walsh et al., 2013). With the rapid development of technology more

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

challenges were introduced to the already complex concept of digital forensics as per Noblett et al. (2000).

In an attempt to encourage organisations to be proactive in achieving digital forensic readiness, pioneers such as Rowlingson (2004) and Kenneally et al. (2005) have sought to demystify the concept of forensic readiness. Their work has provided a base for other researchers to produce models and frameworks that seek to make organisational digital forensic readiness a reality.

Based on Rowlingson's (2004) research, Jordaan et al. (2010) proposed the following as thematic categories, essential to achieving digital forensic readiness:

- i. Strategy;
- ii. Policy and Procedures;
- iii. Technology;
- iv. Digital Forensic Response and
- v. Compliance and Monitoring.

On the other hand, Elyas et al. (2014) take the known thematic categories further by seeking to understand their relationships. They propose a theoretical framework that comprises two main parts, namely:

- i. The state of forensic readiness and the capabilities that characterise forensic readiness and
- ii. Factors that contribute to making an organisation forensically ready.

With this categorisation, Elyas et al. (2014) identify forensic factors as being:

- i. Strategy;
- ii. Top Management Support;
- iii. Governance;
- iv. Culture;
- v. Policy;
- vi. Technical and non-technical stakeholders;
- vii. Training;
- viii. Technology;
- ix. System Monitoring and
- x. System Architecture.

Finally, Elyas et al. (2014) state that these forensic factors collectively interact with the

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

following forensic readiness capabilities:

- i. Legal-evidence management;
- ii. Internal investigations and
- iii. Regulatory compliance.

While not necessarily approached from a broader organisational level, as does Rowlingson's (2004), Jordaan et al. (2010) and Elyas et al. (2014), other noteworthy research relating to digital forensic readiness include those discussed in the next section.

### 2.2.5.1 A Review of Existing Digital Forensic Models

A total of 13 prominent models, which were developed in the 21st Century, were reviewed as part of this study. However, due to the length of the thesis, diagrams and theoretical underpinnings of said models are not included in this Chapter. As can be seen in Table 5, only the model name, year of publication and author are noted. The decision to include models from the period 2001 to 2017 is in line with the research design, as detailed in section 2.2.2 of this Chapter. In addition, this covers a *transitional period* whereby earlier models appear to have been isolated when compared to later models which show attributes of inter-connectedness, as is explained next.

Findings show that in principle, the models reviewed in this study all agree on the key phases of the digital forensic process [1-13]. They attempt to standardise the digital forensic process by defining and refining it [1-13]. Early 21st Century, or traditional models [1-4], attempt to **define** the digital forensic process whilst those ascribed to the latter 21st Century, or modern models [4-13], attempt to **refine** said process. The reviewed models also focus on the **sequence** of the phases in the digital forensic process, thereby making their execution sequential in nature [1-13].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>Period of Model</b>	<b>Name of Model</b>	<b>Model Relationships</b>	<b>Authors</b>	<b>Ref</b>
2001	DFRWS Investigative Model		Palmer (2001)	1
2001	Forensic Readiness		Tan (2001)	2
2002	The Abstract Digital Forensics Model	Derivative of Palmer (2001) <sup>1</sup>	Reith et al. (2002)	3
2003	Integrated Digital Investigation Process		Carrier et al. (2003)	4
2004	Enhanced Digital Investigation Process Model	Derivative of Carrier et al. (2003) <sup>4</sup>	Baryamereeba et al. (2004)	5
2004	A Ten Step Process for Forensic Readiness	Based in Tan (2001) <sup>2</sup>	Rawlingson (2004)	6
2004	A Hierarchical, Objectives-Based Framework for the Digital Investigations Process		Beebe et al. (2004)	7
2009	A Model for Introducing Digital Forensic Readiness to XBRL	Derivative of Rawlingson (2004) <sup>6</sup>	Kotze et al. (2009)	8
2011	Generic Computer Forensic Investigation Model		Yusoff (2011)	9
2012	The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks		Ngobeni et al. (2012)	10
2013	Integrated Digital Forensic Process Model	Derivative of Rawlingson (2004) <sup>6</sup>	Kohn et al. (2013)	11
2014	Digital Forensics as a Service (DFaaS) Process Model		van Baar et al. (2014)	12
2016	On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges		Kebande et al. (2016)	13

Table 5: Digital Forensic Models reviewed.

A key trend noted in some modern models is that they are **context** and use-case specific [5,7-10,13]. A typical example of these are the models by Ngobeni et al. (2012) and Kebande et al. (2016). This means that they are aimed at solving a specific technical problem, such as the analysis of volatile memory data, or a problem within a specific context, such as digital forensics in cloud computing.

Unlike traditional models which were primarily concerned with defining the digital forensic technical process [1-4], more recent modern models [5-13] are **integrated and**



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

**multidisciplinary** in nature. These models start to recognise other stakeholders in the digital forensic process, including concepts such as forensic readiness (Rowlingson, 2004) and the role an organisation plays in the digital forensic process (Kenneally et al., 2005).

### **2.2.5.2 Challenges noted with reviewed models**

While modern models show elements of being integrated, or multidisciplinary in nature, they neither illustrate nor explain the interdependencies between the various stakeholders and/or components across the different disciplines. Findings also show that modern models improve on earlier ones by refining the digital forensic process. However, in so doing they inadvertently end up being more process and/or use case specific. This limits their application within their intended multidisciplinary environment.

This study recognises the contributions of the models, as listed in Table 5, and seeks to provide a truly multidisciplinary and non-sequential approach to organisational digital forensic readiness, taking into account the existing literature, with an aim of illustrating and explaining the interdependencies between the various stakeholders across the different disciplines. Additionally, instead of the core of the model being the digital forensic process, the proposed model seeks to elevate this to digital forensics as a discipline.

### **2.2.5.3 Proposed Model Requirements**

As previously discussed, existing models are context, technology and/or business process specific, and lack the enhanced multidisciplinary approach which seeks to investigate inter-disciplinary interactions.

In line with the problem statement, as derived from literature review, the proposed model intends to address gaps and challenges noted in existing models, with the aim of reducing the organisational risk of inadvertently destroying and negating evidentiary data due to the complexity and multidisciplinary nature of digital crimes. The proposed model was developed through the use of a coordinated, multidisciplinary approach involving both public and private sectors.

The next section unpacks the meaning of what constitutes digital forensics.

## **2.3 An evolutionary practice**

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Over the past decade or so, well-understood procedures and methodologies have evolved within the domain of computer forensics digital evidence collection (Kenneally et al., 2005; Cooper et al., 2010). Kenneally et al. (2005) noted that computer forensic post-mortems are no longer performed on single machines with small storage capacities. Rather, the scope for potential evidence now includes networks of interconnected computers, each with immense storage capacities containing potential artifacts of legal relevance.

This is fast becoming a reality. Garfinkel (2010, p. 64) stated that the “golden Age of computer forensics is quickly coming to an end.” While computer forensic practice is diminishing, a new era of the digital forensic practice is slowly dawning.

In addition, Garfinkel (2010, p. 64) added that “without a clear strategy for enabling research efforts that build upon one another, [digital] forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of computer forensics products will be unable to rely on the results of forensic analysis.”

Many definitions of digital forensics exist. Due to an early saturation point, this section limits the scope to only four definitions from different sources which will be analysed for similarities and differences. The objective is to establish whether available definitions are in harmony and to identify a single definition that can be adopted for the purposes of this study.

The selected process definitions are:

- i. Definition 1: According to Reyes et al. (2007, p. 7) “digital forensics includes preserving, collecting, confirming, identifying, analysing, recording and presenting crime scene information.”
- ii. Definition 2: Reyes et al. (2011, p. 9) explained digital forensics as “the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law.”
- iii. Definition 3: Coopman (2009, p. 1) defined digital forensics as “the collection, examination, preservation and recording of information found on computers and information networks.”
- iv. Definition 4: According to Cooper et al. (2010) digital forensics involve “scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

**2.3.1 Components of the definition**

The common denominator in the definitions discussed is the use of the actual digital forensic *process* as the basis for the definition. Table 6 tabulates the common elements found in each of the four definitions which have been discussed. The uniqueness of each element is reflected by the super-script value appearing at the end of each component.

Definition 1	Definition 2	Definition 3	Definition 4
Preserving <sup>1</sup>	Preservation <sup>1</sup>	Preservation <sup>1</sup>	Preservation <sup>1</sup>
Collecting <sup>2</sup>	Acquisition <sup>2</sup>	Collection <sup>2</sup>	Collection <sup>2</sup>
Confirming <sup>3</sup>			Validation <sup>3</sup>
Identifying <sup>4</sup>			Identification <sup>4</sup>
Recording <sup>5</sup>		Recording <sup>5</sup>	Documentation <sup>5</sup>
Presenting <sup>6</sup>			Presentation <sup>6</sup>
	Analysis <sup>7</sup>	Examination <sup>7</sup>	Analysis <sup>7</sup>
			Interpretation <sup>8</sup>

Table 6: Elements of the digital forensics definition.

As seen in Table 5, while there are commonalities in the elements embedded in each of the four definitions, there are also some differences. These differences and commonalities are discussed further in the next section.

**2.3.2 Gaps in the definitions**

From Table 6, eight unique elements of the definition are found. From this, findings show that elements 1 (*Preserving*) and 2 (*Collection/Acquisition*) are the only explicitly common elements to the four definitions.

Furthermore, definitions 2 and 3 do not possess the same level of detail when compared to definitions 1 and 4. Definition 2 lacks explicit mention of five elements, while definition 3 lacks mention of four. For the purposes of this study, these definitions will therefore be

excluded.

From definitions 1 and 4, findings show six common elements. These are preserving, collecting, confirming, identifying, recording and presenting.

Definition 4 adds further detail by including two additional elements: analysis and interpretation.

### **2.3.3 Propositioned definition**

While all the proposed definitions provide a good understanding of *what* digital forensics is, for the purposes of this study, the definition that best provides clarity is definition 4 by Cooper et al. (2010).

For the purposes of this study, definition 4 was thus adopted in its entirety.

With this definition in mind, the next section explores available literature on digital forensics in order to address the research hypothesis as presented earlier in this chapter.

## **2.4 Findings**

This section investigates the five hypotheses listed in the introduction of this chapter.

### **2.4.1 Hypothesis 1**

The first hypothesis states: *electronic evidence gathered during a digital forensic investigation does not provide sufficient assurance of non-manipulation to the courts.*

As discussed earlier in this chapter, rapid changes and advances in technology and related crimes have necessitated the need to review and improve on digital forensic models and processes. Reyes et al. (2007) also observed that, unlike other forensic sciences, digital forensics theories continue to evolve, as do the techniques.

In the view of recent advances in technology, Bell et al. (2010) argue that it would be imprudent and potentially reckless to rely on existing evidence collection processes and

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

procedures. They added that conventional assumptions about the behaviour of storage media are no longer valid. Unlike traditional storage media, modern storage devices can operate under their own volition in the absence of computer instructions (Kenneally et al., 2005; Chen et al., 2009). Such operations can be highly destructive of traditionally recoverable data. This process has the potential to contaminate evidence and can further obfuscate and hamper the validation thereof (Kenneally et al., 2005).

For the purposes of this study, the use of the term *traditional approaches* denotes forensic procedures undertaken from the dawn of computer forensic practice to 2005 (Kenneally et al., 2005). On the other hand, the use of the term *modern approaches* refers to digital forensic procedures post 2005 (Garfinkel, 2010). As discussed earlier in this chapter, traditional approaches are starting to diminish and, at the same time, modern approaches are being adopted. This period of co-existence of the two approaches affords one a great opportunity to compare these two practices and so appreciate the various strengths inherent in them. This process is explained in detail in the paragraphs that follow. Firstly, we need to explain the basic concept of the traditional approach, also termed *dead forensics*.

### **2.4.1.1 Dead Forensic Acquisition Processes**

To meet the desired goal of preserving original evidence, one of the first steps in traditional evidence collection procedures includes taking the evidence-containing computer system offline and creating a bit-stream image of the entire original evidence disk (Kenneally et al., 2005). Figure 1 presents a summary of the computer forensic process and its objectives according to The Scientific Working Group on Digital Evidence.

The process begins with the preservation of digital evidence by pulling the power cord in preparation for the physical removal of the storage device for imaging purposes. Security becomes an important consideration to ensure the logical and physical safety of the evidence. At the conclusion of the imaging process, a hashing tool is used to authenticate the forensic image. This is then followed by the analysis and reporting phases.

If, during the reporting phase, data is required to be re-authenticated, a cryptographic hash (commonly an MD5 or SHA) is re-calculated to allow parties to show that the data has not changed.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

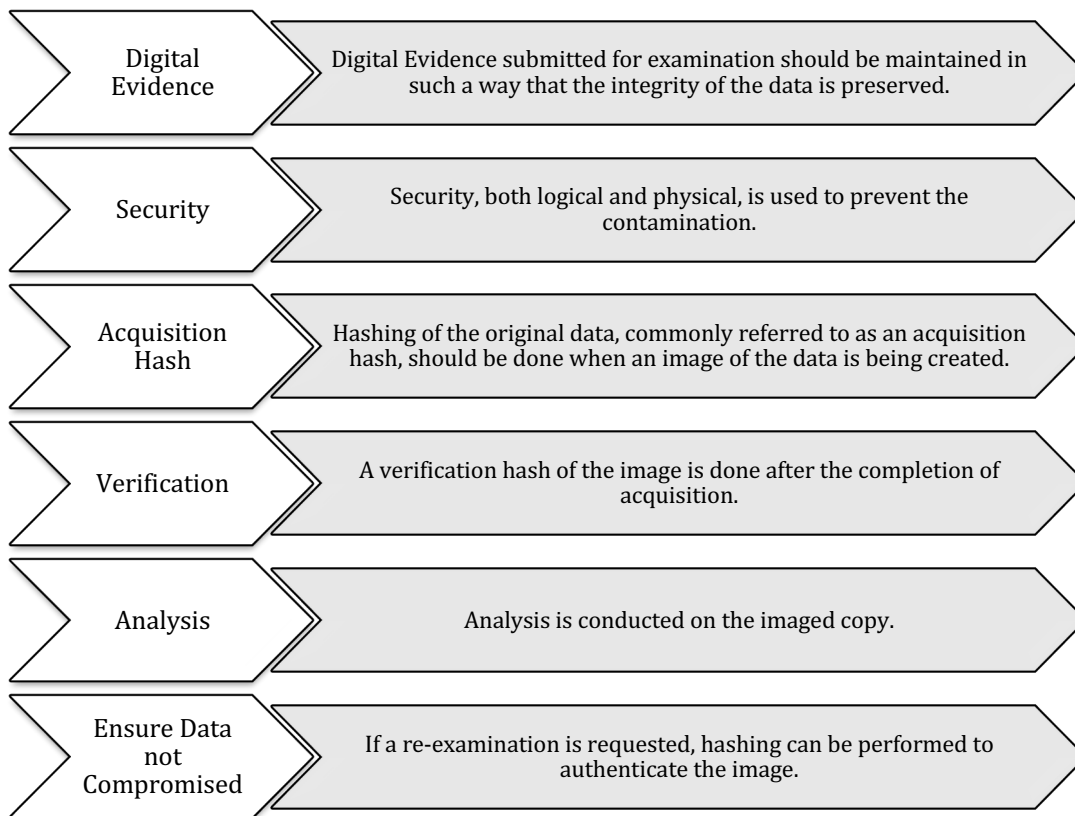


Figure 1: SWGDE Data integrity within computer forensics (SWGDE, 2006).

A change between hash values (suspect/target drive hash vs. destination drive hash) would show that data has been modified and would raise an alarm as to the integrity of the forensic image. The recovery of data must be completed without any data alterations, thereby minimising future challenges during legal proceedings. If a change were to occur, the nature and cause of the change must be explained and described convincingly (Kenneally et al., 2005; Bell et al., 2010).

As discussed earlier in this chapter, the reality is that these well-understood procedures and methodologies have evolved (Cooper et al., 2010; Garfinkel, 2010). The scope for potential evidence has expanded from standalone computers to networks of interconnected computers, each with vast storage capacities containing potential artifacts of legal relevance, making the dead forensic acquisition process increasingly obsolete.

If applied to new storage technologies, dead forensic acquisition processes can negate the post recovery forensic analysis. This challenge is brought about by modern storage devices, such as solid-state drives (SSDs) (Chen et al., 2009; Bell et al., 2010). One can therefore no longer blindly apply dead forensic processes, by pulling the power cord from a computer running a

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

SSD, and assume that evidence will remain intact and unchanged. In addition, the presence of anti-forensic tools on a modern, or traditional drive, can also have the same destructive effect on electronic evidence if the power cord is pulled during computer seizure.

The next section discusses an approach that is being adopted in an effort to counter the limitations of dead forensics.

### **2.4.1.2 Live Forensic Acquisition Processes**

Also known as Fast Forensics, this concept was defined by Reyes et al. (2007) as investigative processes that are conducted within the first few hours of an investigation. As information needs to be obtained within a relatively short timeframe, fast forensics usually involves an onsite/field analysis of the computer system in question.

Live forensic analysis techniques use software that existed on the system during the timeframe being investigated. This is in comparison to dead forensic analysis techniques, which use no software that existed on the system during that timeframe (Carrier, 2006).

Avoiding contamination during the recovery process is paramount and depends on effective, error free data recovery from digital devices. Traditionally, write-blocking hardware combined with bit-stream image copying processes served this purposes. Some live forensics techniques utilise Linux or other forensic boot disks to perform on scene/site searches and data extraction. The boot disks run in memory only and mount the hard drives as read only so as not to corrupt the evidence (Reyes et al., 2007).

Live forensic analysis focuses on preserving and analysing volatile data. Volatile data is any data that is stored in memory, or in transit, which will be lost when the computer loses power, or is powered off. It resides in registers, cache and Random Access Memory (Adelstein, 2006; Sutherland et al., 2008).

Sutherland et al. (2008, p. 65-73) argue that there is no way to avoid making changes, since in order to conduct a live examination it is necessary to deploy tools on the live system to capture data, and such tools will make changes to the running system.

This argument was later supported by Chan et al. (2010) who ascertained that current forensic tools are limited by their inability to preserve the hardware and software state of a system

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

during investigation. Existing tools can overwrite evidence present in memory, or alter the contents of the disk causing forensic taint which, in turn, lowers the integrity of the evidence.

On the other hand, taking a snapshot of the system can result in a phenomenon known as *forensic blurriness* where an inconsistent snapshot is captured because the system is running while being observed. Forensic blurriness affects the fidelity and quantity of evidence acquired and can cast doubt on the validity of the analysis, resulting in the court's increased reluctance to accept such evidence (Chan et al., 2010).

Although forensic techniques can collect significant amounts of vital information, investigators are weary of anti-forensic techniques which can hide, or intentionally obfuscate information gathered, thus affecting the veracity and fidelity of the evidence collected (Wiles et al., 2007; Chan et al., 2010).

We can conclude that both dead and live forensic acquisition processes do not provide sufficient assurance of non-manipulation. This proves the first hypothesis to be correct. Therefore, if existing computer forensic procedures ultimately render evidence inadmissible, then the need for a redefinition of the methodology is paramount.

The next section discusses the digital forensic process.

### **2.4.2 Hypothesis 2**

The second hypothesis states: *there is a lack of standardisation in the criteria against which electronic evidence is validated as no consistent digital forensic methodology exists.*

Studies suggest that while many processes have been defined for both live and dead forensics, there remains a lack of a common standardised process (Hoolachan et al., 2010; Hunton, 2010). This section discusses the related literature and draws a conclusion based on the findings.

#### **2.4.2.1 Global lack of standardisation**

In a study conducted by Rogers et al. (2004), findings indicated that both the law enforcement community and the private sector/academia are concerned with the lack of a standardised, or even a consensus approach, to the training of computer forensics practitioners. The latter was



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

found by Taylor et al. (2007) and Hoolachan et al. (2010) to have a negative impact on an organisation's forensic readiness. The concept of *forensic readiness* is discussed later in this chapter.

Hunton (2010) acknowledged that there are many rigorous and robust cybercrime and digital investigation models already in existence that can provide valuable guidance and structure. However, many of these models focus on the recovery of digital evidence from already identified technology. On the other hand, they are abstract in nature and lack direct support and alignment to the broader needs of law enforcement investigations.

In addition, Coopman (2009) stated that until now, most law enforcement agencies have tailored their computer forensic responses to meet their individual departmental needs. This is a challenge experienced by most organisations offering digital forensic services. Hoolachan et al. (2010, p. 33) also found that "the digital revolution has profoundly affected how both private and law enforcement organisations handle digital evidence." Hence, digital forensic practices and the handling of digital evidence is an issue pertinent to many organisations, not just in South Africa, but throughout the world.

### **2.4.2.2 Standardisation: A South African perspective**

In South Africa, the issue of a common standard is being investigated extensively by a Cyber Forensic Forum, formed by the Association of Certified Fraud Examiners SA (ACFE SA, 2011). This forum also found that many organisations, including law enforcement, approach digital forensic investigations based on their own internal processes as there is no common standard. Some of the standards being reviewed by this Forum are listed in Table 7.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>Abbreviated Name</b>	<b>Full Organisation Name</b>	<b>Document Title</b>
CSIR	Council for Scientific and Industrial Research	Process Flows for Cyber Forensics Training and Operations
DFCB	Digital Forensics Certification Board	DFCP/DFCA – KSA Domains (v1.3)
IACIS	International Association of Computer Investigative Specialists	Certification Competencies (v 2)
IOCE	International Organisation for Computer Evidence	Guidelines for Best Practice in the Forensic Examination of Digital Technology (Draft v1.0)
SWGDE	Scientific Working Group on Digital Evidence Standards	Best Practices for Computer Forensics (v 2.1)
SANAS	South African National Accreditation System	Criteria for Laboratory Accreditation in the field of Forensics (TG 01-01)
ACPO	Association of Chief Police Officers	Good Practice and Advice Guide for Managers of e-Crime Investigation: Managers Guide (v 0.1.4)

Table 7: ACFE SA reference resources for the creation of a common digital forensic standard in South Africa.

The ACFE SA Cyber Forensic Forum has identified the lack of a common digital forensic standard as a challenge and has embarked on a mission to formulate one. From this we can conclude that the second hypothesis, which states that *there is a lack of standardisation in the criteria against which electronic evidence is validated as no consistent digital forensic methodology exists*, is true. With the first hypothesis also having proven true, this adds further severity to the enormous risk the digital forensic practice faces.

The next section discusses the third hypothesis which investigates the impact of various advances in technology on the practice of digital forensics.

### **2.4.3 Hypothesis 3**

The third hypothesis states: *forensic technology for gathering digital evidence is increasingly lagging behind the advances being made in anti-forensic tools and the rapid changes in storage technology.*

As previously mentioned, the traditional concept of dead forensics has for many years been accepted and practiced in the computer forensic field. According to Bell et al. (2010), the long-established and accepted procedures cover situations such as the automated recovery of court-submissible evidence which a defendant has previously attempted to delete. Indeed, the peculiarity of *deleted, but not forgotten* data which so often comes back to haunt defendants in court is in many ways a bizarre artefact of hard drive technology. This stems from the reality that traditional hard disks have slow access speeds relative to their capacity for storage. The latter makes complete erasure very inconvenient, and from the fact that there is no performance penalty incurred for writing over existing data (which makes complete erasure unnecessary).

This situation is in the process of changing (Garfinkel, 2010). Newer technologies, such as the Solid-state drives (SSD), are much faster and more complex. However, these complexities are not limited to only SSDs, but extend to other storage forms such as Raid Arrays, Storage Area Network (SAN) and Network Attached Storage (NAS) devices as well.

For purposes of explaining these challenges in detail, this chapter only elaborates on the changes in storage systems, as they apply to the SSD.

#### **2.4.3.1 Basic Operation of a Solid-state drive (SSD)**

SSDs operate by storing data in (typically) 512kb blocks, subdivided into (typically) 4kb pages. These pages/blocks are comprised of large arrays of Negative-AND (NAND) digital logic. These NAND transistors are, in essence, very similar to the NAND logic chips used to build computer processor units (CPUs). They have an extra gate, known as a floating gate, which is used to *trap* charge (to store charge on an extremely limited scale as a capacitor might). This arrangement is stable and can allow microscopic quantities of charge to be stored for years without leakage and without requiring a supply of power. The term *solid-state* refers to the fact that the data is stored in fixed arrangements of electronic transistors which are, in turn, part of fixed materials. These transistors can be read to in tens of microseconds and written to in hundreds of microseconds, which compares very favourably with hard disks, whose latency for read/writes is usually 3 - 10 milliseconds, i.e. 30 - 3 000 times slower. Chen et al. (2009) and Bell et al. (2010) offer a detailed explanation of the technical functionality of an SSD.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

As SSD drives fill up, even a change to a single byte may result in an entire block needing to be read/erased and rewritten, resulting in an overt slowdown in performance. Many manufacturers have therefore added routines to the drive controller chip that can pre-emptively act to ameliorate the *reset* problem. One common strategy is known as *Garbage Collection* or ‘Self-Healing’. The underlying philosophy is to cautiously identify areas that are not in use, and to then reset them as soon as possible.

If garbage collection were to take place before (affecting *dead forensics*) or during (affecting *live forensics*) forensic extraction of the drive image, it would result in irreversible deletion (or *corrosion of evidence*) of potentially large amounts of valuable data that would ordinarily be gathered as evidence during the forensic process.

We can thus conclude that advances in storage technology are bringing about new challenges to the digital forensic practice domain. The next section discusses the threat of anti-forensic tools to the practice of digital forensics.

### 2.4.3.2 Anti-Forensic Tools

According to Doherty et al. (2008), an increasing number of private investigators are declining various digital forensic investigation work because the required tools are very expensive and have a short lifespan. This is mainly as a result of the increasing and changing variety of digital devices available on the market each year.

Commensurate changes that need to be made in the forensic tool manufacturers to accommodate or address new file systems, operating systems and connectivity demands also contribute to the short lifespan of forensic tools. Doherty et al. (2008) ascertained that in the United States of America (USA) many municipal law enforcement personnel face challenges as their departments cannot justify the acquisition of expensive tools (with a short lifespan) that may, or may not, work with seized devices in lawful investigations.

The issue of tools and other technical resources becomes even more pertinent as anti-forensic efforts continue to increase. Anti-forensics can be defined as “the movement to exploit weaknesses in the forensic process or tools” (Reyes et al., 2007, p. 246). It can also involve various acts of hiding data from the forensic examination. Older techniques were as basic as running a simple script to perform a touch command on every file to alter file attributes (*date and time stamps*), or deleting log and temporary files (Wiles et al., 2007).

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

While one may still encounter these types of anti-forensic measures, other tools and techniques have emerged that are far more sophisticated. This section discusses only a few of these to provide a basis for positioning the extent to which anti-forensic measures have advanced.

Table 8 illustrates a sample of available anti-forensic tools and describes their functionality.

The rising surge of anti-forensic tools and their ease of access on the internet directly impacts on an organisation's ability, or lack thereof, to effectively respond to digital crimes (Taylor et al., 2007).

If one explores the risks which an organisation are exposed to if not forensic ready, Casey (2006, p. 48-55) comments that "sophisticated intruders take full advantage of the lack of forensic readiness. To respond more effectively to such attacks, computer security professionals and digital forensic investigators must combine talents and work together. The ability to apprehend sophisticated perpetrators depends in large part on the ability of investigators to follow the cyber trail left by the culprits."

Some functionality offered by security products have a dual function. Intrusion detection systems (IDSs), centralised logging and forensic software are some examples of software tools that are deployed to detect an incident and which can also gather evidence in subsequent phases as part of forensic readiness (Khurana et al., 2009). While the latter is true, the hypothesis that *forensic technology for gathering digital evidence is increasingly lagging behind the advances being made in anti-forensic tools and the rapid changes in storage technology* is true. There is a need to find a balance between the functionality that security applications provide (e.g. secure deletion) and the reverse engineering capability required from digital forensic tools.

Findings show that security applications have advanced far beyond digital forensic tools, rendering some forensic tools obsolete against (anti-forensic) actions undertaken using security tools.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>Anti-Forensic Tool</b>	<b>Source Website</b>	<b>Description</b>
Evidence Eliminator	<a href="http://www.evidence-eliminator.com/">www.evidence-eliminator.com/</a>	Commercial tool for secure deletion. While it can be used to protect company intellectual property, this tool can also be used to destroy evidence.
Metasploit	<a href="http://www.metasploit.com/">www.metasploit.com/</a>	Offers penetration testing tools. Includes a suite of tools to secure data. These tools can also act as anti-forensic applications.
Sam Juicer	<a href="http://downtown.trilo.de/svn/downloads-20080101/_20081011-0601_metasploit-antiforensics_/20081011-0602_www-metasploit-com---antiforensics.mht">http://downtown.trilo.de/svn/downloads-20080101/_20081011-0601_metasploit-antiforensics_/20081011-0602_www-metasploit-com---antiforensics.mht</a>	A Meterpreter module that dumps the hashes from the SAM file. While this is a good feature for investigations, it can be used to illegally gather data from the SAM file.
Slacker	<a href="http://www.forensickb.com/2007/10/encrypt-to-detect-use-of-slackerexe.html">http://www.forensickb.com/2007/10/encrypt-to-detect-use-of-slackerexe.html</a>	Allows a user to hide files within the slack space of the NTFS file system. This being an anti-forensic practice.
Timestamp	<a href="http://www.anti-forensics.com/tag/timestompexe">www.anti-forensics.com/tag/timestompexe</a>	Allows you to modify all four NTFS timestamp values: modified, accessed, created and entry modified. Thereby altering the integrity of data.
The Defiler's Toolkit	<a href="http://www.securitywizardry.com/index.php/products/forensic-solutions/anti-forensic-tools/the-defiler%27s-toolkit/visit.html">http://www.securitywizardry.com/index.php/products/forensic-solutions/anti-forensic-tools/the-defiler%27s-toolkit/visit.html</a>	Toolkit consisting of a pair of tools that allow a more secure deletion of files on UNIX systems. The same set of tools can be used to destroy evidence.
Transmogrify	<a href="http://www.blackhat.com/.../bh.../BHUS09-Blunden-AntiForensics-PAPER.pdf">www.blackhat.com/.../bh.../BHUS09-Blunden-AntiForensics-PAPER.pdf</a>	Tool to defeat forensic tools' file signaturing capabilities by masking and unmasking your files as any file type. A common anti-forensic practice.
Window Washer	<a href="http://www.webroot.com/En_US/consumer-products/windowwasher.html">http://www.webroot.com/En_US/consumer-products/windowwasher.html</a>	Commercial tool for secure deletion. While it can be used to protect company intellectual property, this tool can also be used to destroy evidence.

Table 8: A sample of modern anti-forensic tools and their functionality.

This challenge presents an opportunity, not only for new forensic tools, but also for the enhancement of the overall digital forensic model. This will be further discussed in the chapters that follow.

The next section investigates the validity of the fourth research hypothesis as presented earlier in this chapter.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **2.4.4 Hypothesis 4**

Hypothesis 4 states: *individuals involved in the digital forensic investigation and prosecution process are not sufficiently trained and/or educated.*

#### **2.4.4.1 Education, Training and Certification**

Firstly, a distinction between education, training and certification is required. Cross (2006) stated that “education is generally measured by tenure: you spent a day in the seminar or four years in college. Training, on the other hand, is measured by what you can do when you've completed it.”

Certification, in the ICT world, involves the extensive testing of a person's abilities in their area of specialisation (Schlichting et al., 2004). With this in mind, this section explores the impact of education, training and certification of digital forensic practitioners.

#### **2.4.4.2 Impact of human resource limitations**

In a study conducted by Rogers et al. (2004), findings show that education, training and certification were the most reported inherent challenges in computer forensics. This is consistent with the findings from the previous law enforcement study conducted by Stambaugh et al. (2001). The study also ascertained that both the law enforcement community and the private sector/academia, are concerned with the lack of a standardised, or even a consensus approach, to training computer forensics practitioners. As previously mentioned, Hoolachan et al. (2010) are of the opinion that this can negatively impact the organisation's Forensic Readiness.

One of the main strengths of Rowlingson's (2004) forensic readiness model is the recognition of the range of personnel within an organisation who can become involved in a legal inquiry (Taylor et al., 2007; Hoolachan et al., 2010). This model identifies no less than eleven different departments and their associated personnel that must be considered in an investigation.

Although the variety of staff involved generally varies, depending on the magnitude of the investigation, Hoolachan et al. (2010) argue that there are a multitude of people who need to understand the correct protocol within a digital investigation.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Venter (2006) found the situation in South Africa regarding the need for education, training and certification similar to how Rogers et al. (2004) explained it. According to Venter (2006), candidates with adequate technical background and training are not always available or retainable and he adds that the training of Cyber First Responders is therefore a challenge.

Venter (2006) further stated that in order to meet the requirement to expand the Cyber Forensics capability within the South African government, training in Cyber Forensics was necessary. He attributes complications to the lack of sufficient resources with a background or formal training in ICT.

From the above findings, the hypothesis that *the people involved in the digital forensic investigation and prosecution process are not sufficiently trained and/or educated*, is therefore proven to be true. As it will become evident in the section that follows, this inadequacy of human resources directly impacts not only on the admissibility of evidence, but also on the forensic readiness of an organisation. The next section explores the concept of forensic readiness in more detail.

### **2.4.5 Hypothesis 5**

Hypothesis 5 states: *an organisation responding to a digital crime, without an incident response plan, may take actions that compromise the admissibility of evidence to a court of law.*

As Reith et al. (2002) point out, that which leads to the prevalence of cybercrimes in today's world, is the reality that there is a small chance of ever being caught. This means that in order to catch and prosecute criminals involved in such a crime, investigators need to employ consistent and well-defined forensic procedures (Campbell, 1998; Page, 2002).

Moreover, countless instances of computer crimes around the world remain vastly underreported (Obuh, 2011; Gershowitz, 2011) as victims fear the exposure of vulnerabilities, the potential for copycat crimes and the loss of public confidence (McConnell International, 2000). Gershowitz (2011) adds that private firms, concerned with the potential negative publicity or that proprietary information may be required by investigators, are particularly hesitant to report computer crimes.

Rowlingson (2004, p. 1) defines forensic readiness "as the ability of an organisation to



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

maximise its potential to use digital evidence whilst minimising the costs of an investigation.” Garcia (2005, p. 6) later modified this definition to state forensic readiness as the “art of maximising the environment's ability to collect credible digital evidence.”

From the perspective of law enforcement agencies, the forensic process begins when the crime has been committed, or when a crime has been discovered and reported. The concept of forensic readiness, according to Hoolachan et al. (2010), is that an organisation can pre-empt the occurrence of a crime by gathering evidence in advance and in doing so, organisations will benefit not only in instances where prosecution becomes an issue, but also in limiting their own business risks.

The business requirement to gather and use digital evidence has been recognised in a number of studies. Rowlingson (2004) notes that enterprise policies can enhance computer and network forensics. In addition, they propose six categories of policies to facilitate digital forensic investigations. Their categories are designed to help organisations deter computer crime and position themselves to respond to successful attacks by improving their ability to conduct investigations. The six categories of policies that facilitate digital forensic investigations are:

- i. Retaining Information – Policies that relate to the storage of information by an organisation;
- ii. Planning the Response – Policies that guide the organisation’s plans to respond to various incidents and situations;
- iii. Training – Policies that address the training of staff members and those affiliated to the organisation;
- iv. Accelerating the Investigation – Policies that address operational aspects of investigations;
- v. Preventing Anonymous Activities – Policies that address the organisation’s proactive efforts against the risk of fraud and
- vi. Protecting the Evidence – Policies that address the handling and protection of evidence and other vital data.

While these underline the importance of cohesion of policies in an organisation, the problem with the categorisation, as proposed by Rowlingson (2004), is that an organisation needs to have six policies in place and this may result in possible duplication and/or conflicting policy statements. Furthermore, the latter may lead to confusion in identifying the authority/governing policy regarding the facilitation of digital investigations. As an alternative, a central point of

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

reference (policy) would therefore best serve the purpose of communicating the organisation's position on digital forensic investigations.

From the above discussion, the concept of *forensic readiness*, as explained by Rowlingson (2004), was found to have two main objectives:

- i. Maximising an environment's ability to collect credible digital evidence and
- ii. Minimising the cost of forensics during an incident response.

While policies are important, they alone will not guarantee an organisation's overall forensic readiness. An implementation plan (incident response) must be developed and tested. The next section discusses this plan and how it should be developed in order to enhance the organisation's digital forensic readiness.

### **2.4.5.1 Incident Response Plan**

According to Jaatun et al. (2009) incident response is the process of responding to security-related incidents involving information and communications technology infrastructure. Incident response has traditionally been rather reactive in nature, focusing mainly on technical issues (Shinder et al., 2008; Jaatun et al., 2009). An incident can be anything from an attack that crashes all the servers and cuts off all network communications to an intrusion that causes no actual damage, but demonstrates the vulnerability of the organisation's systems (Shinder et al., 2008; Lillard et al., 2010).

According to Taylor et al. (2007) although all security incidents should be taken seriously, they do not all have the same severity. An Incident Response Plan should therefore define *how* incident severities will be determined and *what* this means in terms of incident handling.

### **2.4.5.2 Incident Management**

David (1999) suggests that prior to dealing with the incidents that have been deemed worthy of treatment, there are three significant points that should be made. *Firstly*, all events should be logged, and the logging should be in as much detail as possible. This makes allowance for things, such as later treatment of the non-priority items, detecting patterns leading up to incidents and a ready source of information regarding events that are action items.

The *second* important step is that there should be an escalating set of responses, when and if

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

appropriate. The benefits derived from this step are what can be called *quick and dirty* initial reactions to certain incidents, providing follow-up actions if the earlier ones fail to accomplish their goals. *Lastly*, David (1999) suggests that events, including those not selected as incidents to be treated in the incident response plans, should be treated with reasonable promptness.

If the above steps are not taken to stop events of lesser importance, those initiating these events can continue doing them without fear of reprisal, and they might even try more severe attacks (David, 1999; Lillard et al., 2010).

### **2.4.5.3 Response Team**

In an attempt to be proactive, many organisations form incident response teams, called Computer Incident Response Teams (CIRTs). These teams are made up of trained individuals whose goal it is to react speedily to occurrences of incidents (Lamis, 2010).

Each team member is responsible for a pre-assigned area, thus decreasing the amount of damage and increasing the likelihood of apprehending the perpetrator of the incident (Shinder, 2008; Jaatun et al., 2009). An Incident Response Manager, whose responsibility includes coordinating notifications, escalations as well as ensuring that the incident response team is properly assembled, usually leads this team (Taylor et al., 2007).

Lamis (2010) added that communication between team members, including external stakeholders, is essential to creating a resourceful environment to effectively combat and handle incident responses.

Research suggests that building a response team should involve many different organisational departments such as legal and public relations (Taylor et al., 2007; Lamis, 2010). These additional parties sometime include external parties who provide support and possess skills that may not be present in the organisation. These external parties should also be readily available to assist internal teams in the event of an incident (Shinder, 2008; Lillard et al., 2010).

We can thus conclude that the hypothesis that *an organisation responding to a digital crime without a forensic readiness plan, will take actions that compromise the admissibility of evidence*, is true. This means that while there may be a desire to be forensically ready within the organisation and in relation to evidence gathering, there is also a need for forensic readiness

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

amongst all staff members.

### 2.5 Conclusion

The goal of this chapter was to investigate hypotheses 1 to 5, utilising a systematic literature review as a research method for the investigation process. This chapter and demonstrated the use of a systematic literature survey. The chapter concluded with a discussion of the 5 hypotheses investigated, which can be summarised as follows:

Hypothesis 1: During this section we discussed traditional and modern approaches to digital forensics, including the evolution of computer forensics. The result of this discussion was the finding that *existing digital investigation methodologies (Live and Dead forensic acquisition processes) do not provide sufficient assurance of non-manipulation of evidence*. The study found that the latter is due to the rapid changes/advances in storage technologies.

Hypothesis 2: In this section we investigated literature relating to standardisation in the digital forensic profession. Findings show that the *digital forensic industry lacks standardisation in the criteria used for collecting evidence*, which has resulted in a lack of innovation synergy, limited regulation and misalignment of education and certification relating to digital forensics. This as a result of the various legal systems, which have varying requirements.

Hypothesis 3: Here we discussed the impact of recent advances in storage technologies on existing digital forensic processes. This section demonstrates that a trade-off exists between the functionality of information security and digital forensic tools. Findings show that *forensic technology for gathering evidence is increasingly lagging behind* due to rapid advances in anti-forensics and changes in technology and this is negatively impacting on the successful prosecution of electronic crimes.

Hypothesis 4: In this section we explored Education, Training and Certification as three distinct concepts. The findings show that *people involved in the digital forensic process are not adequately trained and educated*, thereby contributing to the inadvertent destruction of evidentiary data.

Hypothesis 5: Here we explored the concept of *forensic readiness* and the factors that have an impact on it. Findings show that *a mature technical environment alone is not the only factor impacting on the organisation's forensic readiness, and that without an incident response plan,*

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

*an organisation will take actions that compromise the admissibility of evidence.* In addition, the study found that existing literature does not define the concept of *digital forensic readiness* sufficiently well for it to be implemented and, that it also lacks a framework to guide said implementation.

In the light of all the research hypotheses having been proven true, we can conclude that there is a need to revisit the underlying principles of digital forensics. This further highlights the need for a multidisciplinary digital forensic model, geared particularly at addressing challenges faced by law enforcement and corporates in developing economies.

### **3. Chapter 3: Research Design**

---

#### **3.1 Introduction**

This chapter presents the research design adopted for this study, and the justification thereof. It begins with a discussion of the research approach and then explains the ontology, epistemology and the different paradigms considered in this study which is followed by the justification of the choice of the different research methods and their associated data gathering and analysis methods. The next section discusses the research design.

#### **3.2 The Research Design**

This research adopts a post modernistic approach, a philosophical position which proposes that reality is constructed within belief systems, and that the observer is an integral part of what is being observed (Kvale, 1992; Bergmann, 2011). This approach was found appropriate as the researcher is a digital forensic practitioner, and as such, an integral part of this research process.

On the contrary, positivism science adheres to the view that only factual knowledge, gained through observation and measuring, is trustworthy (Weber, 2004; Teddlie et al., 2009). In positivism studies the role of the researcher is limited to data collection and interpretation. Research findings garnered from such an approach are observable and quantifiable (Kvale, 1992). Since most of the data collected for this research is qualitative in nature, this approach was not found to be suitable.

Similarly, a post normal science approach was *not* adopted as its strength is in the management of complex science-related issues (Funtowicz et al., 2003). It focuses on aspects of problem solving that tend to be neglected in traditional accounts of scientific practice: uncertainty, value loading and a plurality of legitimate perspectives (Funtowicz et al., 2003; Weber, 2004).

The application of said research approach was based on Kyrö's (2014) outline of the paradigm and methodological choices in scientific research. See Figure 2 for a graphical representation of the paradigm and methodological choices. This also formed a foundation for the thinking process adopted during the development of the M-DiFoRe Model.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

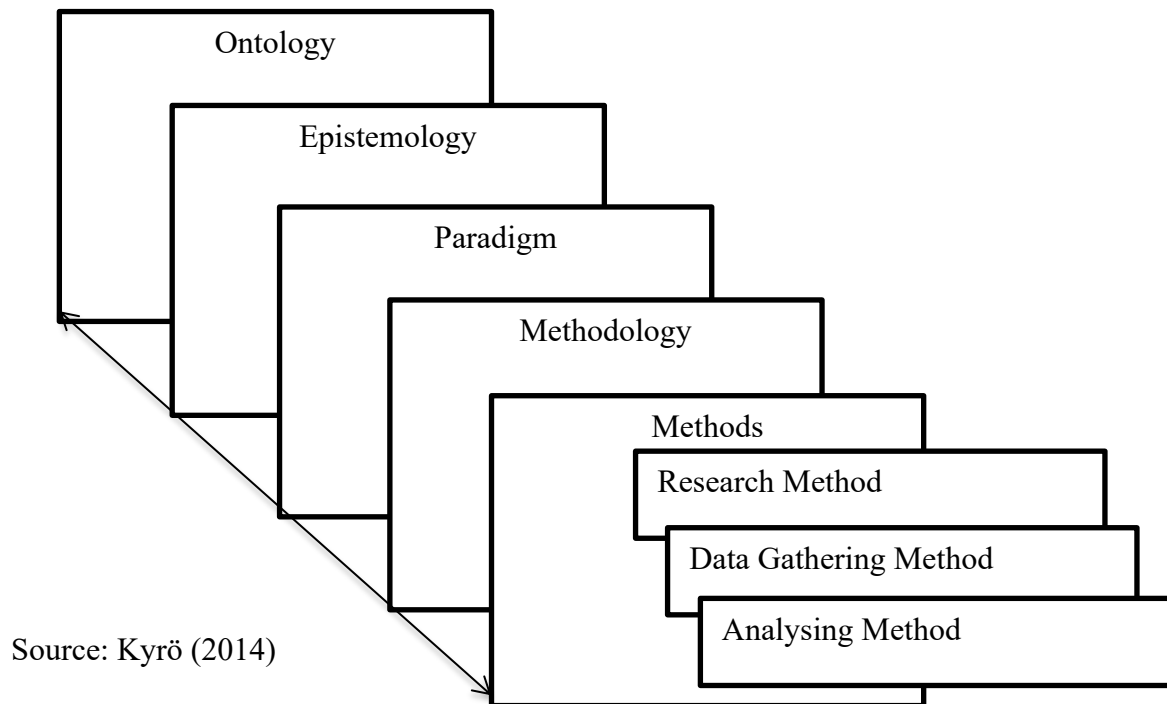


Figure 2: The paradigm and methodological choices in scientific research (adapted).

The next section presents the theory behind each layer of the research process, discusses the application thereof in this study and provides an outline of the thesis.

### 3.2.1 Ontology

Philosophical assumptions and beliefs about reality form our ontology (Mitchell, 2005). According to Morgan (2007) and Mack (n.d), ontology can be thought of as one's view of reality, or as Kyrö (2014) suggests, ontology refers to ideas of reality and how it is constituted.

The practical application of ontology in research is that one cannot study something one does not believe exists. Kyrö (2014) added that “the essential questions of how we believe that what we believe exists can be: do we believe that what exists is stable or do we believe that it changes, or is it unique or universal and what is the relationship between human existence and the world?”

This study considered the critical realist and relativist ontologies as the main contrasting positions. According to Levers (2013, p. 2), “critical realism is a contemporary uptake of the realist ontological perspective that reality exists independent of the human mind regardless of whether it is comprehensible or directly experienceable.” On the other hand, Levers (2013) added that relativist ontology is the belief that reality is a finite subjective experience and

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

nothing else exists outside of our thoughts. Reality from a relativist perspective is not distinguishable from the subjective experience of it.

This study was undertaken based on the view, or belief, that organisational digital forensic readiness can be achieved through a multidisciplinary approach, which seeks to understand inter-disciplinary interactions between key stakeholders. As the latter delves into the subjective views of stakeholders, and forms the basis for the development of the M-DiFoRe Model, the relativist ontology applies.

### **3.2.2 Epistemology**

According to Morgan (2007) and Mack (n.d), epistemology relates to *how* one acquires knowledge. Kyrö (2014) also added that epistemology is interested in *how* we can acquire knowledge about reality.

Weber (2004) asserts that positivists view reality as separate from the individual who observes it, or in other words, the subject (the researcher) and object (the phenomena in the world that are their focus) are two separate, independent things. To achieve this, positivists generally rely on qualitative data to investigate social issues (Weber, 2004). On the other hand, interpretivists believe that reality and the individual who observes it cannot be separated and that reality is subjective and based on meanings and understanding (Weber, 2004; Mitchell, 2005).

This study adopts the epistemological view that the *reality* or belief (ontology) under investigation needs to be interpreted, rather than measured, in order to discover the underlying meanings and activities associated with the inter-disciplinary interactions between key stakeholders involved in the digital forensic readiness process. Furthermore, that the subject and object of this research are not dualistic in nature, and as such, the interpretivist paradigm applies as the data used is of a qualitative nature. The latter is discussed in the sections that follow.

### **3.2.3 Paradigm**

According to Kyrö (2014), a paradigm “is manifested as a group of theories and definitions suitable for describing the field of study, or in a large the phenomenon and a group of methods, suitable for studying this field.” Levers (2013) argues that it is imperative for researchers to choose a research paradigm that is congruent with their beliefs regarding the nature of reality.



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

This section presents literature which relates to the use of five paradigms namely: the transformative, pragmatic, integrated, post positivist, interpretivist and constructionist research paradigms. It concludes with a justification for the paradigm adopted in this study.

### **3.2.3.1 Transformative paradigm**

The 2007 National Science Board's report on Enhancing Support of Transformative Research at the National Science Foundation (NSB-07-32) defined transformative research as "research driven by ideas that have the potential to radically change our understanding of an important existing scientific or engineering concept or leading to the creation of a new paradigm or field of science or engineering. Such research is also characterised by its challenge to current understanding or its pathway to new frontiers" (NSB, 2007, p.v).

### **3.2.3.2 Pragmatic paradigm**

On the other hand, pragmatism focuses on the *what* and *how* of the research problem, it places the research problem centrally and applies all approaches to understanding the problem, and it is not committed to any one system of philosophy or reality (Creswell, 2011). Armitage (2007) proposes that since research is often multipurpose, adopting a "what works" tactic will allow the researcher to address questions that do not sit comfortably within a wholly positivistic or interpretivist paradigm.

Mackenzie et al. (2006) added that early pragmatists rejected the scientific notion that social inquiry "was able to access the truth about the real world solely by virtue of a single scientific method." Pragmatism places emphasis on abduction, inter-subjectivity and transferability (Morgan, 2007). This creates new opportunities for thinking about classic methodological issues in the social sciences:

- i. **Abductive Reasoning:** the pragmatic approach is to rely on a version of abductive reasoning that moves back and forth between induction and deduction. Here the inductive results from a qualitative approach can serve as inputs to the deductive goals of a quantitative approach, and vice versa.
- ii. **Inter-subjectivity:** a researcher has to work back and forth between various frames of reference in order to achieve a sufficient degree of mutual understanding with, not only the people who participate in our research, but also the colleagues who read and review the products of our research.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

- iii. Transferability: We cannot simply assume that our methods and approach to research make our results either context-bound or generalisable; instead, we need to investigate the factors which affect whether the knowledge gained can be transferred to other settings.

### 3.2.3.3 Integrated paradigm

Hall (2012) argues that while transformative and pragmatic paradigms remain amongst the most dominant in mixed methods research, these single paradigms do not provide an adequate rationale for mixed methods research. Furthermore, Hall (2012) proposes that for mixed methods research, a realist or integrated perspective is needed to overcome inherent limitations found in the said single paradigms.

Regarding the limitations of single paradigms, Bergmann (2011) suggested that the ideal would be a paradigm that does not limit the range of topics researched, nor the methods that can legitimately be used to conduct research.

When applying this paradigm, one can adopt a scientific realist ontology in the conduct of evaluation (Pawson et al., 1997). Alternatively, one can adopt an emergent realist ontology, in which Henry et al. (1998) argue that the objective of said views of reality is best aided by a combination of quantitative and qualitative methods.

Mingers (2001) and Jones (2000) noted that there are inherent problems when attempting to mix philosophical approaches. These include *cultural barriers* (the QUAL approaches are more commonly employed by EU research groups, while North American researchers lean towards the QUAN approaches), *psychological barriers* (a lack of expert support regarding unpopular approaches can lead to reduced confidence and create psychological barriers) and *practical barriers* (single-method research is a tried and tested approach, with literature and experts readily available while, on the other hand, establishing coherent philosophical foundations for an integrated approach can prove to be a time-consuming exercise, making it impractical to adopt this approach).

It is with the previous in mind that Zachariadis et al. (2010) propose critical realism as a middle way to address challenges associated with the mixing of philosophical approaches. It simultaneously confronts the challenges posed by both the natural and social science regimes,

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

making critical realism significantly relevant to IS research as it addresses technological characteristics (natural science) which exist within an organisation (social science) (Mingers, 2004; Zachariadis et al., 2010).

### **3.2.3.4 Post positivist paradigm**

According to Levers (2013), this paradigm accepts that truth and universal laws exist but that the discovery of these truths is near impossible. Post positivists expect to progress closer to the truth while recognising that discoveries are only partial segments, or approximations, of truth (Levers, 2013). As a result of its critical realist ontology, the post positivist paradigm accepts that knowledge is fallible as it is shaped by contextual influences (Zachariadis et al., 2010; Levers, 2013).

### **3.2.3.5 Interpretivist paradigm**

The interpretivist paradigm is said to be conceptualised as having a relativist ontology with a subjectivist epistemology, and is aligned with postmodern thought process (Levers, 2013). This suggests that interpretivist research relies on the researcher's set of beliefs about the world. The interpretive paradigm's key focus is the recognition and narration of the meaning of human experiences and actions (Mingers, 2004; Levers, 2013).

### **3.2.3.6 Constructionist paradigm**

According to Levers (2013, p. 3), the constructionist paradigm is "conceptualised as having aspects of both the post positivist and interpretivist paradigms - ontological critical realism with epistemological subjectivism. Meaning is created through an interaction of the interpreter and the interpreted. The interpreter, though not entirely objective, is separate from the phenomena to be observed and the meaning-making interaction is strongly influenced by the phenomena and society. Knowledge of the observed is constructed rather than discovered."

### **3.2.3.7 The Paradigm Adoption Rationale**

This research adopts the interpretivist paradigm for the following reasons:

- i. The study adopted a relativist ontology together with a subjectivist epistemology, a combination which is best suited for the interpretivist paradigm.
- ii. The subject and object of this research are not dualistic in nature, and as such the

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

interpretivist paradigm applies.

iii. The data used in this study is primarily of a qualitative nature.

### **3.2.4 Methodology**

Weber (2004, p. 100) proposes that methodology is tied to ontology and epistemology in that “given the nature of reality and beliefs about knowledge of that reality, it shows how to generate new knowledge that is consistent with the epistemology and ontology.” At this level, a methodology provides a systematic and theoretical analysis of the methods applied to a field of study (Levers, 2013).

The above suggests that the way in which one views the constructs of reality and knowledge, affects how one will set about uncovering knowledge regarding relationships among the noted phenomena and social behaviour, and how one evaluates one’s own and other’s research (Mackenzie, 2006; Morgan, 2007; Mack, n.d).

Patel (2015) states that methodology answers the question: “What procedure can we use to acquire knowledge?” He further proposes that in order to remain consistent with the relativist ontology and the interpretive paradigm, grounded theory can be adopted as an appropriate methodology.

Charmaz (2014) added that grounded theory methodology is amongst the most influential and widely used modes for carrying out qualitative research, especially when the researcher’s principle aim is to generate theory.

As explained in justifying the choice of ontology and epistemology, this study seeks to discover the underlying meanings and activities associated with the inter-disciplinary interactions between key stakeholders involved in the digital forensic readiness process. As such, grounded theory was adopted as methodology as it allowed for the use of research methods that aided in achieving the research objectives. The latter (research methods) is discussed in the next section.

As part of the process of applying grounded theory, a systematic literature review was conducted (Chapter 2), along with an analysis of interviews (Chapter 3) and case law data (Chapter 4). A qualitative research tool was used to facilitate the coding, analysis and interpretation (Chapters 3 to 7) of said interviews and case law data. This led to the generation

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

of new theory, the M-DiFoRe model, and its workings.

### **3.2.5 Research Method**

Patel (2015) states that *method* answers the question: “What tools can we use to acquire knowledge?”

Since this study has adopted the epistemological view that the *reality* or belief (ontology) under investigation needs to be interpreted, rather than measured, and assumes a relativist ontology with a subjectivist epistemology, the method of choice is qualitative in nature. The choice of a qualitative research method is consistent with the subjectivist epistemology and relativist ontology (Patel, 2015).

The use of a systematic literature review (Chapter 2), along with an analysis of interviews (Chapter 4), facilitated the theoretical triangulation necessary to strengthen the grounded theory results (Yin, 2011). As Craig (2009) and Yin (2011) explain, the triangulation process involves the application of different methods on different types of data. The said triangulation was successfully applied and completed, and is detailed in section 4.4 of this thesis.

### **3.2.6 Data Gathering Method**

Creswell (2011) and Patel (2015) argue that qualitative research provides for varying data gathering methods which include, but are not limited to interviews, observation, case study, focus groups, action research and ethnography.

Data gathering methods affect the quality, quantity, adequacy and appropriateness of data and are dictated by practical considerations such as the nature of the research problem, cost (time and money), availability of data and access to it (Pawar, 2004).

This study employs a pluralistic approach to data gathering through the application of a systematic literature review, interviews and case studies as methods to investigate the problem statement. The interviews conducted provided a means to capture current views of industry experts, as they relate to pertinent aspects of this research. A review of case law added a pragmatic perspective to the issues being investigated and facilitated the theoretical triangulation necessary in grounded theory methodologies; the result being the formation of a foundation upon which the M-DiFoRe model was developed.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **3.2.7 Analysing Method**

As Miles et al. (1994, p. 12) stated, the “strengths of qualitative data rests very centrally on the competence with which their analysis is carried out.” They further added that the qualitative data analysis method consists of three concurrent flows of activity, namely:

- i. Data reduction: refers to the process of selecting, focusing, simplifying, abstracting and transforming source data. When applied, it means deciding on which data to code, and which to exclude, and identifying patterns that are meaningful for further reflection.
- ii. Data display: refers to “an organised, compressed assembly of information that permits conclusive drawing and action.” Examples of this include newspaper headlines and summary dashboards. These help us understand what is happening and prompt us to either analyse further, or take another action, based on our understanding.
- iii. Conclusion drawing/verification: takes place during, and after analysis, and is comprised of meanings that emerge from the data.

Qualitative data analysis is a continuous and iterative process which needs to be documented in order to facilitate reflection and usability by others (Miles et al., 1994; Craig, 2009).

To meet the requirements of a qualitative data analysis method, this study used Atlas.ti which, as Friese (2012) explained, is computer software for qualitative analysis of large bodies of textual and multimedia data, designed to explore complex phenomena hidden in data, and facilitate the reduction, display and conclusion drawing process. The application of the analysis method and process is detailed in section 3.2.6. Appendices 5, 6, 7 and 8 of this thesis serve as auditable records to confirm the output generated using Atlas.ti, and to facilitate reflection and usability by others.

### **3.3 Conclusion**

The purpose of this chapter is to present the research methodology that was used in this study, and to motivate as to why the specific approaches were adopted. The chapter presented the ontology and epistemology used, along with the research paradigm of choice. It further expands on the methodology, research method, data gathering method and analysing method selected.

As discussed in section 1.4 of this study, it was necessary to use different research methods in

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

order to strengthen grounded theory results. This chapter therefore positioned how a literature review, along with interviews would be used as research methods to facilitate the triangulation of results.

The chapter concludes with a mention of Atlas.ti, which was used as a quantitative data analysis tool. The details of how the said tool was applied are found in the specific chapters where analysis took place.

The next chapter uses interviews as a research method to gather real life experiences and opinions of South African industry experts regarding the various hypotheses stated. This chapter also includes the coding, analysis and interpretation of said interview data, using Atlas.ti.

## **4. Chapter 4: Data Gathering And Analysis**

---

### **4.1 Introduction**

This chapter continues with testing the research hypotheses presented in Chapter 1. Unlike Chapter 2, which made use of a systematic literature review to test the hypotheses, this chapter adopts a different approach in that interviews are used as the data gathering method to investigate hypotheses 6 to 10. This course was adopted to validate findings, drawn from the literature survey, with the real-life experiences of South African digital forensic practitioners.

Interviews are a data gathering method which involve one person (the interviewer) posing questions to another person (the interviewee). Research suggests that interview questions may be open-ended, closed ended, or both (Teddlie et al., 2009; Creswell et al., 2011). Both types of questions were used in this study, largely because they provided ample opportunity for the interviewer to ask for further explanations of vague answers and to provide clarification where a question was not clear (Teddlie et al., 2009). This was particularly important as the interviewees hailed from different industries and had different personalities.

The 5 hypotheses being investigated are:

- i. Hypothesis 6 (H6): South African organisations do not need to concern themselves with digital forensic readiness, as digital crimes are not commonplace.
- ii. Hypothesis 7 (H7): The Electronic Communications and Transactions (ECT) Act of South Africa adequately positions the acceptable use of, and extent to which, electronic evidence can be used in a civil or criminal proceeding.
- iii. Hypothesis 8 (H8): South Africa has a standardised digital forensic model and process which is used by authorities to investigate and prosecute digital crimes.
- iv. Hypothesis 9 (H9): As a result of the presence of the electronic laws in South Africa, the prosecution of digital crimes faces no limitations.
- v. Hypothesis 10 (H10): Those individuals involved in the prosecution of digital crimes are knowledgeable, adequately trained and professionally certified.

This chapter commences with a discussion regarding the way in which interviews were used in this study as a data gathering method. The core of this chapter is a discussion of the results



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

garnered from the interview process, which includes a discussion on the coding process of interviews as well as the analysis and interpretation of coded data. The chapter concludes with a summation on the results of the five hypotheses discussed.

### **4.2 Data Gathering Method**

The next section discusses interviews as a data gathering method used to further test the hypotheses.

#### **4.2.1 Choice of Interview Types**

Patton (2002) defined four types of open-ended interviews, ranging from the least structured (informal conversational interview) to more structured (general interview guide approach) to most structured (standardised open-ended interview). He also described the closed fixed-response interview but did not advocate its use. Below is a summary of Patton's four types of interviews:

- i. Type 1: Informal conversational interview – Questions emerge from the immediate context and are asked in the natural course of things; there is no predetermination of the question topics or wording.
- ii. Type 2: General interview guide approach – Topics and issues are specified in advance, in outline form; interviewer decides sequence and working of questions in the course of the interview.
- iii. Type 3: Standardised open-ended interview – The exact wording and sequence of the question are determined in advance. All interviewees are asked the same basic question in the same order. Questions are worded in a completely open-ended format.
- iv. Type 4: Closed fixed-response interview – Questions and response categories are determined in advance. Responses are fixed; respondent chooses from amongst those fixed responses.

For purposes of this study, a mixture of Type 1 and Type 3 open-ended interviews was used. Teddlie et al. (2009) state that researchers employing the INT-QUAL strategy may use one of the open-ended interview approaches, as described by Patton (2002). He also noted that it is possible to combine the interview types. His suggested sequence of qualitative interview techniques, as used in this study, is as follows:

- i. Start with the unstructured informal conversational interview approach, which can be used to build a rapport and elicit spontaneous responses;

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

- ii. Move on to the interview guide approach that provides a more comprehensive outline of topics, yet maintains a conversational tone and
- iii. Finish with the highly structured, standardised open-ended interview approach, which greatly increases response comparability.

For the purposes of this study, the structure followed was to begin with an unstructured informal conversational interview approach, followed by a highly structured, standardised open-ended interview approach. The latter formed the core of the interview, while the unstructured, informal conversational component was mainly used to build a rapport with the interviewees.

The next section contains the application of the interview method in designing the interview questions.

### **4.2.2 The Interview Instrument**

The questions, as contained in Appendix 3, were designed using the method discussed in the previous paragraph (The Research Method). Questions were designed to address the five hypotheses, as presented earlier in this chapter.

### **4.2.3 The Interviewees**

This section discusses the criteria followed in order to select the interviewees, the communication channels used in conducting the interviews and the ethical considerations underscoring the interview process.

#### **4.2.3.1 Interviewee Selection Criteria**

The interviewees were selected based on the following criteria:

- i. A multidisciplinary selection of individuals from the Legal, Business/Private Sector and Law Enforcement disciplines;
- ii. Individuals with experience in digital law and/or digital forensics and
- iii. Individuals who have been involved in digital forensic investigations in South Africa for a period of no less than three years.

These criteria were used to ensure that the interviewees would provide a mixture of opinions

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

from varying experiences gained in different working environments. In line with UNISA's ethics guidelines, as discussed in Chapter 1, consent letters were sent to the interviewees. See Appendix 4 for a template of the blank consent letter.

The sample size was limited to 7 respondents, who led national digital forensic teams from within the public and private sector. To ensure quality and accuracy of results, it was decided to limit respondents to national team leaders, rather than operational staff, as they could provide insight into decisions affecting policy and strategy. Given the design and research objective of this study, this number of respondents was found to be acceptable and appropriate as it yielded the desired quality data (Scott, 2005).

### **4.2.3.2 Communication Medium**

As discussed earlier, studies have shown that while open-ended interviews traditionally occurred face-to-face, they may also take place over the telephone and via the Internet (Crichton et al., 2003; Teddlie et al., 2009; Salmons, 2010).

A total of seven interviews were conducted using the following three ways:

- i. Face-to-face (4);
- ii. Via telephone (1) and
- iii. Via email (2).

The reasons for using three different approaches were:

- i. Where possible, the first preference was to conduct face-to-face interviews. This was especially important where the researcher had little or no prior knowledge of the interviewees.
- ii. The interviewees resided in different and wide-spread geographical locations within South Africa. In order to conveniently and timeously access the interviewees, email and telephone were used as contact methods.
- iii. Lastly, given the interviewees' seniority in their respective organisations, it was not always possible to conduct face-to-face interviews. In order to maintain open discussions and constant contact (and thus keep interviewees interested in the study), telephone and email communication mediums were used.

### **4.2.4 Ethical Considerations**

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

To ensure structure and adherence to good research ethical practices, an ethical clearance was obtained from UNISA. This clearance procedure takes an in-depth approach to ensuring that the research is conducted in ways which uphold the university's ethical policies.

In addition, prior to the commencement of the interview process, each interviewee signed a consent form to indicate his/her willingness to participate in the research process. This documentation is stored for a period of five years, as stipulated by UNISA's research guidelines.

The ethical considerations, identified as being directly relevant to the interview process, were the protection of the autonomy of participants, obtaining informed permission from the gatekeepers/employer and the protection and disposal of sensitive data/samples obtained from the interview.

The above countermeasures were taken to address the identified ethical concerns:

- i. The protection of the autonomy of participants was done by the use of an informed consent form, which specifies all relevant facts relating to the research being undertaken.
- ii. A consent form was also used to ensure that the interview participants, where necessary, obtain permission from their employers to participate in the interview.
- iii. All information obtained during the interview was stored in a secure facility and additional security measures, such as encryption and access control, were used to protect this data from unauthorised access for a period of five years, as required by the university. At the end of this time electronic files will be securely deleted and physical records shredded.

In conclusion, the logic and relevance of the research instrument content was pre-checked by a digital forensic expert and this resulted in changes being made to some of the questions. The final revision of the research instrument was then double-checked by both the researcher and research supervisor. In addition, the final interview instrument was submitted to UNISA's ethical committee for approval.

### **4.3 Analysing Method**

This section discusses the method used to analyse interview data.

#### **4.3.1 The Data Analysis Tool**

To thoroughly analyse the data gathered during the interviews, an appropriate tool was needed

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

to facilitate the analysis process. Whilst this process could be done manually, based on the volume of data gathered during the interview process, it would prove to be a tedious process. It was therefore necessary to find a tool that would:

- i. Assist in the process of identifying and making sense of the opinions and perspectives expressed in the interviews;
- ii. Assist in the correlation and analysis of the different sources of information and
- iii. Allow the researcher to retain control and methodological freedom from hypotheses testing to grounded theory.

The research tool selected for this purpose was Atlas.ti (Atlas.ti, 2011). This product is described as one of a new generation of qualitative data analysis software packages which can be used to analyse interviews, field notes, textual sources and other types of qualitative data. It offers different licensing models for various applications (Casasempere, 2007; Contreras, 2011; Friese, 2011). For the purposes of this study, a student license was obtained.

### **4.3.2 The Data Analysis Process**

The coding process began with the creation of a Hermeneutic Unit (HU) within the Atlas.ti application. The HU can be best described as a “container that holds the sources of information of all of the analytical work done around them” (Contreras, 2011). The tool requires that every research project is assigned an HU *holding* the sources of information to be analysed.

For the purposes of this study, the Hermeneutic Unit created contained the following objects:

- i. Primary documents: This comprised the consent form and other physical documents obtained from the interview participants. In addition, electronic recordings of the interviews were also included as primary documents in the project HU.
- ii. Quotations, Codes, Memos, Networks and Families: This is data generated from the transcribed interviews during the analysis process.

#### **4.3.2.1 Quotations**

Once the HU was created, the first step was to load each primary document for analysis. During this process, *Quotations* were created. These quotations were segments of the text, from the transcribed interviews, which were selected and deemed interesting for further analysis. The quotations created varied from single words to complete paragraphs. Once all the quotations

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

were created, they were semantically analysed across the different primary documents and hyperlinks were created to identify patterns of similar concepts.

### **4.3.2.2 Codes**

The patterns of similar concepts were then further marked as *Codes* within Atlas.ti. Codes are “concepts that can either drive from frameworks or reference or emerge from the text” (Contreras, 2011). Once codes were formed in each primary document, and across the various transcribed interviews, they were further correlated into one to identify shared conceptual characteristics. The result of this process is the formulation of what this thesis later refers to as *Components* of the M-DiFoRe model.

### **4.3.2.3 Memos**

A further Atlas.ti feature which was used during this study is *Memos*. This feature allows for reflections or commentaries (in the form of notes) to be made on quotations and codes. For the purposes of this study, commentaries were made on the shared conceptual characteristics derived from individual codes and quotations. These memos are embedded in each code and quotation, and were used in this thesis to serve only as a means to jot the researcher’s notes and/or comments on key points to remember about each code or quotation.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

### 4.3.2.4 Families

In order to organise the shared conceptual characteristics found, *Families* of codes were created by grouping related codes together and assigning a name to each group. This was a critical step towards the interpretation of data and the linking of findings of this process towards the objectives of the study. The result of this process is the formulation of what this thesis later refers to as *Domains* of the M-DiFoRe model.

### 4.3.2.5 Networks

Once the families were created, data could be interpreted in full. This phase entailed the use of HU *Networks* that Atlas.ti automatically created from the codes and families that were created during the analysis phase. These networks are a graphical representation of the coded data and they depict the relationships between the codes and families created.

The above process is graphically summarised in Figure 3.

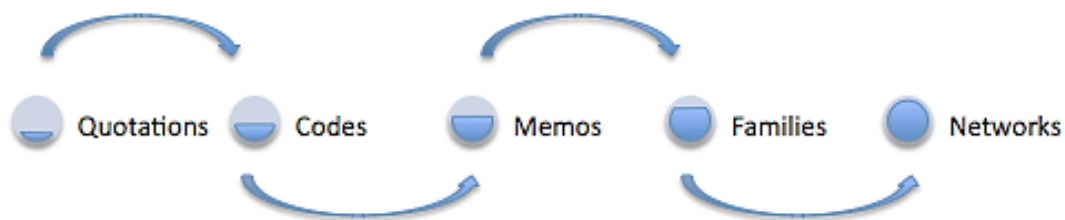


Figure 3: Data analysis process summary using Atlas.ti

For evidence of the application of the above process refer to Appendix 5, the HU report generated by Atlas.ti.

## 4.4 Findings

This section presents the profile of the interviewees, discusses how the data analysis method was applied and presents results from the analysis process.

### 4.4.1 Interviewee Profiles

Table 9 presents a summary of the seven interviewee profiles, where INT1 is the abbreviation used to denote the first interviewee and INT2 the second interviewee, and so forth. Table 9

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

also shows an evaluation of the interviewees in relation to the selection criteria presented earlier in this chapter.

<b>Interviewee</b>	<b>Experience &gt; 3 Years</b>	<b>Law Enforcement</b>	<b>Private Sector Experience</b>	<b>Management Position</b>
INT1	Yes	Yes	No	Yes
INT2	Yes	Yes	Yes	Yes
INT3	Yes	No	Yes	Yes
INT4	Yes	Yes	Yes	Yes
INT5	Yes	No	Yes	Yes
INT6	Yes	Yes	No	Yes
INT7	Yes	Yes	Yes	Yes

Table 9: Summary of interviewee profiles.

Findings show:

- i. All interviewees had industry experience in excess of the required three years;
- ii. Five of the seven interviewees had law enforcement experience;
- iii. Five of the seven interviewees had private sector experience; and
- iv. All interviewees held a managerial position.

Owing to the executive levels held by the respondents in their respective organisations, a sample size of 7 respondents was accepted as it was sufficiently representative of the digital forensic community in South Africa (Mathews, 2010).

The iterative coding process made it possible for focus/immersion to be applied to each individual question, and for the emergence and crystallisation of themes to take place. Differences in findings (codes and themes) between the interviewees were also resolved using said iterative process.

#### **4.4.2 Interview Responses**

The questions were aligned with the five hypotheses which, in turn, were aligned with the research objectives and literature themes, as depicted in Table 10.



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>Literature Themes</b>	<b>Research Objectives</b>	<b>Hypothesis</b>	<b>Interview Questions</b>
Technical and Legal Challenges	RO1	H6	Q6, Q10, Q15
Digital Forensic Methodology	RO2	H7	Q5, Q7, Q11
Digital Forensic Advances	RO3	H8	Q8, Q9, Q4
Human Resource Management	RO4	H9	Q12, Q13, 14
Digital Crime Preparedness	RO5	H10	Q1, Q2, Q3

Table 10: Summary of the relationship between hypotheses 6 to 10, interview questions and related research objectives.

This section describes the results of the seven interviews. Questions were not asked sequentially as this would hamper the natural flow of the conversation (interview). See Appendix 3 (Interview instrument) which details Questions 1 to 15, as asked during the interviews.

#### **4.4.3 Hypothesis 6**

Hypothesis 6 states: *as a result of the presence of the electronic laws in South Africa, the prosecution of digital crimes faces no limitations.* The following interview questions were asked to garner opinions which would help investigate this hypothesis:

- i. Does electronic evidence provide sufficient assurance of non-manipulation (Q6)?  
*Respondents were of the opinion that the law makes it possible for electronic evidence to be relied upon.*
- ii. What are the factors that contribute to electronic evidence being rendered inadmissible (Q10)? *Respondents pointed to digital forensic processes and procedures as a good foundation for ensuring the admissibility of evidence.*
- iii. What do you think should be done to increase the prosecution rate of digital crimes in South Africa (Q15)? *Responses included special courts, education, training, certification, focused research, development of law and defined models and processes.*

The above findings suggest that the hypothesis is not true, as a lack of processes, procedures, education, training and certification can act as limitations during the prosecution of digital crimes.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

### 4.4.4 Hypothesis 7

Hypothesis 7 states: *South Africa has a standardised digital forensic model and process that is used by authorities to investigate and prosecute digital crimes.* The following interview questions were asked to gather opinions that would help investigate this hypothesis:

- i. Do you, or your organisation, have a digital forensic model which has been adopted (Q5)? *Respondents indicated that they use their own entity-specific model, which may differ from those used by other organisations.*
- ii. Is there a standard process for electronic evidence gathering (Q7)? *Respondents indicated that, while processes adopted in their individual organisations were similar, no process standards specific to South Africa exist.*
- iii. Have you noted any challenges that prevent digital crime investigators from correctly applying the digital forensic model or framework (Q11)? *Respondents indicated that a single point of reference was needed. Other points noted were that South Africa needs a specific model, which must enable and support legal processes, and that this model must be flexible.*

Findings suggest that the hypothesis is not true, as no single common model or process is in place within the South African legal context.

### 4.4.5 Hypothesis 8

Hypothesis 8 states: *The Electronic Communications and Transactions (ECT) Act of South Africa adequately positions the acceptable use of, and extent to which electronic evidence can be used in a civil or criminal proceeding.* The following interview questions were asked to gather opinions that would help investigate this hypothesis:

- i. Does the law adequately position the acceptable use of/or extent to which electronic evidence can be used in civil or criminal proceedings (Q8)? *Respondents stated that the law (ECT Act) makes it possible to present electronic evidence in a South African court of law. However, contradictions were noted in responses as some respondents felt that existing laws support the ECT Act, while others felt that discrepancies exist between the ECT Act and existing laws.*
- ii. Does the law cater for the complexities of modern IT devices (Q9)? *Respondents indicated that the law lagged behind technology. While the ECT Act was regarded as strong legislation, respondents suggested that it was in need of periodic review.*
- iii. Have you noted any challenges regarding the prosecution of digital crimes (Q4)?

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

*Challenges noted included the lack of knowledge regarding digital forensic principles among the stakeholders, a lack of understanding of legal requirements and a lack of resources.*

Findings suggest that this hypothesis is true, as the ECT Act makes it possible to present electronic evidence in a court of law.

### 4.4.6 Hypothesis 9

Hypothesis 9 states: *those individuals involved in the prosecution of digital crimes are knowledgeable, adequately trained and professionally certified.* The following interview questions were asked to garner opinions that would help investigate this hypothesis:

- i. Do you think digital forensic investigators are sufficiently trained to do their work (Q12)?  
*Respondents identified a need for more training for local digital forensic investigators.*
- ii. Have you noted any challenges that prevent prosecutors from successfully prosecuting digital crimes (Q13)? *Respondents identified challenges to include a lack of interest in digital crimes, high caseloads, a lack of digital forensic training and/or awareness and a lack of cooperation amongst stakeholders.*
- iii. Do you think state prosecutors are sufficiently trained to do their work (Q14)?  
*Respondents opined that a need to train state prosecutors exists.*

Findings suggest that this hypothesis is not true, as credentials were noted as being a general limitation amongst prosecutors and investigations alike.

### 4.4.7 Hypothesis 10

Hypothesis 10 states: *South African organisations do not need to concern themselves with digital forensic readiness, as digital crimes are not commonplace.* The following interview questions were asked to gather opinions that would help investigate this hypothesis:

- i. Should South African organisations be concerned about digital crimes (Q1)? *Responses included varying opinions, pointing to views that digital crimes were on the increase. The intangible nature of data in electronic format causes people to lower their defences; modern criminals are technologically literate and have access to good legal representation; the immaturity of the digital forensic profession allows criminals to go free and following correct investigative processes to preserve evidence is important.*
- ii. Which three types of digital crimes do you find to be the most prevalent (Q2)? *Responses*

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

*indicated: financial crimes, child pornography, hacking and illegal access, malware-related crimes, 419 scams and Internet misuse.*

- iii. Which sector do you find to be the most targeted (Q3)? Respondents listed the following sectors: banks/financial sector, large corporates, private individuals, mining sector and general businesses/corporates at large.

This hypothesis was proven untrue as findings point to a prevalence of various types of digital crimes.

With the exception of number eight, all other hypotheses were proven untrue. The next section discusses how the above information was interpreted, based on the coding process that took place using Atlas.ti.

### 4.5 Interpretation of Findings

As previously discussed, this study made use of Atlas.ti to code and analyse interview data.

Figure 4 shows the resulting network map of the coded data. To achieve the results presented in this section, all interviews were transcribed and each transcript repetitively read in order to identify codes for each question answered by the participants.

From Figure 4, three code families are noted: Corporate Environment (with six codes), Industry Environment (with three codes) and Legislative Environment (with three codes).

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

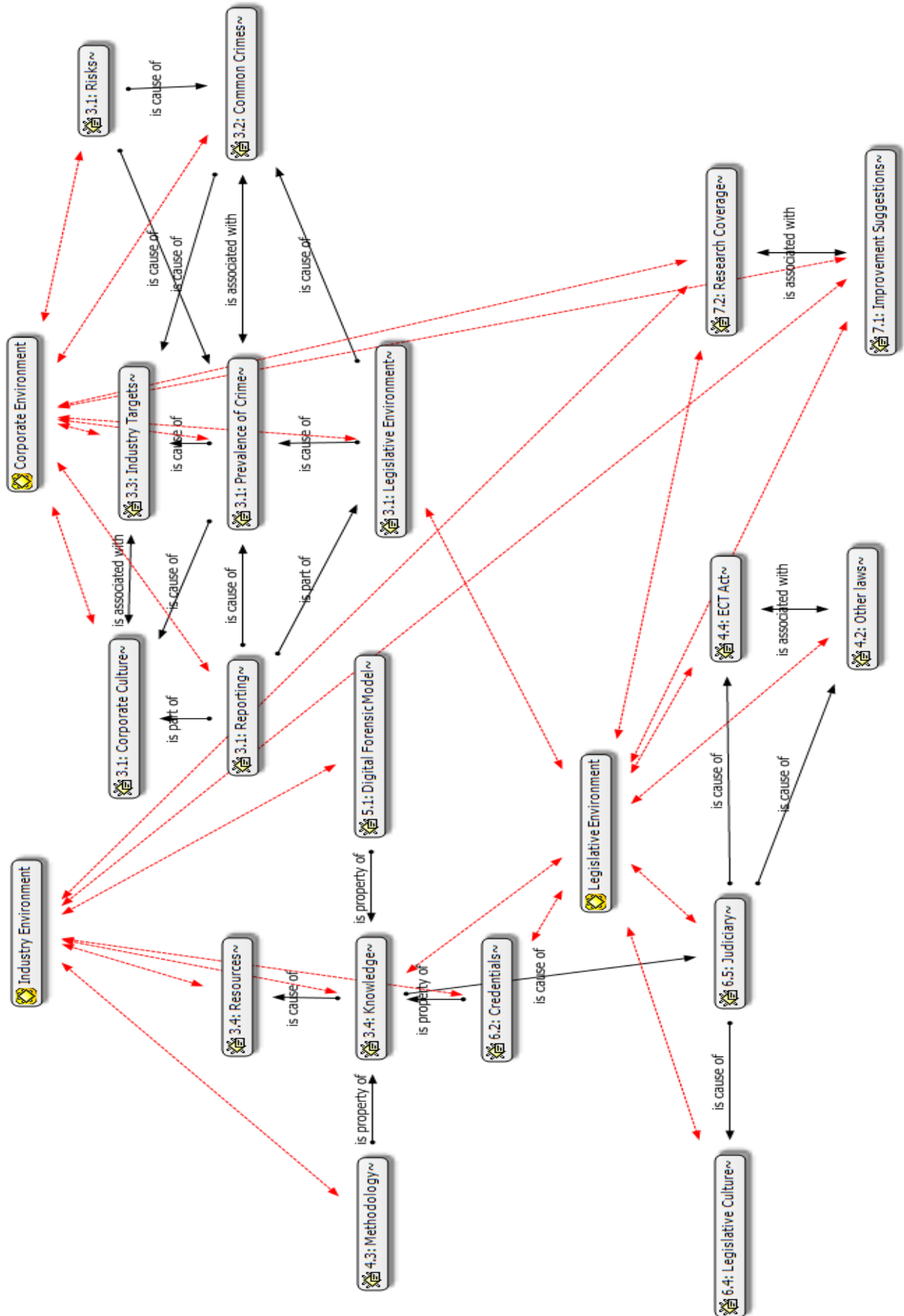


Figure 4: Summary of network maps formed from analysis of interview data.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

Techniques from both immersion/crystallisation and constant comparison (grounded theory) were applied in order to assist with the interpretation and development of the initial and final codes. These codes resort under each of the said environments (Borkan, 1999; Corbin et al., 2008).

Findings relating to the codes and families are discussed next.

### 4.5.1 Corporate Environment

For the purposes of this study, the corporate environment is defined as *comprising of juristic persons who participate and contribute to the economy*.

A total of six codes (corporate culture, reporting, industry targets, prevalence of crime, risks and common crimes) were identified and classified into a common code family. Key findings from the correlation of results from each interview revealed the following:

- i. Corporate Culture: A large proportion of organisations were found to have a habit/culture of ignoring/overlooking small crimes. A general lack of governance, policies and procedures, as regards fraud risk management, was found to exist. Additionally, a lack of resources (human and financial) was also noted. Finally, a lack of awareness (digital crime prevention and detection) was also identified.
- ii. Reporting: The reporting of digital crimes was found to be low. Reasons identified for this included the culture of ‘sweeping things under the carpet’, a lack of education, ignorance and the lack of effective Law Enforcement.
- iii. Risks: The following risk areas were identified:
  - a. The intangible aspect of technology causes people to lower their defences. This is evident in the various types of white-collar crimes committed using technology.
  - b. Modern IT criminals are technologically literate and possess financial, and other resources, including access to good lawyers.
  - c. Advances in mobile technology innovations pose a risk as criminals are quick to exploit them.
  - d. The digital forensic industry is not fully matured, enabling criminals to take advantage of loopholes in global legal structures.
  - e. DFIs, not following due process, contribute to the low prosecution rate of digital crimes.
- iv. Prevalence of crime: Findings show that the number of digital crimes is on the increase. Those affected are all current, and future, users of technology. The high prevalence of

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

crime is also attributed to legal gaps. These will be discussed later under the topic, Legislative Environment.

- v. Common crimes: The following crimes were identified as common across all industries affected by digital crimes:
  - a. Child Pornography;
  - b. 419 Scams;
  - c. Wire/EFT fraud;
  - d. Asset misappropriation;
  - e. Card skimming;
  - f. Malware related crimes;
  - g. IP theft;
  - h. Illegal access and
  - i. Internet misuse.
- vi. Industry targets: It was generally conceded that criminals target organisations where there is a perceived big gain. These targets are mainly situated in the financial services sector and include large corporations. Lastly, individuals were also ascertained to be easy targets.

### 4.5.2 Industry Environment

For the purposes of this study, the industry environment is defined as *a branch of economic or commercial activities relating to digital forensics*.

The code family, Industry Environment, contains three codes namely Knowledge, Credentials and Methodology which relate to the Corporate Environment family of codes. Key findings from the correlation of results from each interview revealed the following:

- i. Knowledge: Knowledge was found lacking amongst those involved in the investigation value chain, including prosecutors, judges, industry experts and private as well as public sector organisations. Training of all stakeholders was noted as essential. Specific weight was placed on legal requirements as superseding technical processes. It was found that industry experts lacked an understanding of legal requirements and were not correctly applying their technical knowledge. The lack of clear policies and processes contribute to the latter.
- ii. Credentials: Lack of cohesion between the academic sphere and industry was identified. While interviewees noted that no single qualification served as a prerequisite to qualify

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

as an industry expert, the need for specialised training and the maintaining of a balance between education and experience were determined necessary. A digital forensic model was also deemed essential towards guiding the required training.

- iii. Methodology: While various versions of methodologies exist, the need for a single point of reference was noted. This extended to the need for consistency in country specific (*South African*) standards, processes and a digital forensic model. The absence of such was identified as an inhibiting factor to the prosecution of digital crimes. An open culture of information sharing, was noted, would serve to promote the maturity of the digital forensic profession. Specific to a digital forensic model, this would not be considered a law, but rather a *guideline* as it would enable and support the legal process, while remaining flexible enough to accommodate advances/changes in the law and/or technology. Lastly, awareness of academic models, and the alignment of the correct methodology and digital forensic model to the appropriate law, was identified as being necessary.

### 4.5.3 Legislative Environment

For the purposes of this study, the legislative environment is defined as *a branch of commerce that is responsible for drafting and enforcing laws*.

The last code family to emerge from the iterative coding process is that of the Legislative Environment. This comprises three codes: Legal culture, Judiciary and the ECT Act/Laws.

- i. Legal culture: Findings show a lack of interest in digital crimes among prosecutors and judges. A lack of cohesion between law enforcement and the prosecuting authorities was also noted. The disinterest was attributed to possible high caseloads and limited resources. A mind-shift is needed if this culture is to change. Training and awareness making were suggested as effective drivers of this change. In addition, the study ascertained that the creation of special interest groups and special courts could introduce positive reforms.
- ii. Judiciary: Findings suggest that the judiciary is presented with two problems which result in a reluctance to prioritise on digital evidence - high caseloads and a lack of knowledge (DF processes and methodologies).
- iii. eCrime Law: Specific to the South African laws on electronic evidence (ECT Act), findings show the key strengths of the law to be that it is a strong piece of legislation which provides a good baseline. On the other hand, findings indicate that some suggest that the law has low penalties, lacks awareness, is not well understood by many and is



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

overly complex in its use of technical terminology. Lastly, the ECT Act, written to cater for the next 10 to 20 years of technological advances, was perceived as satisfactorily.

This information can be tabulated in the following way:

<b>Corporate Environment</b>	<b>Industry Environment</b>	<b>Legislative Environment</b>
Corporate Culture	Knowledge	Legal culture
Reporting	Credentials	Judiciary
Risks	Methodology	eCrime Law
Prevalence of crime		
Common crime		
Industry targets		

Table 11: Code themes developed from analysis of interview data.

Table 11 was derived through the application of techniques extracted from both immersion/crystallisation and constant comparison (grounded theory) to assist with the interpretation and development of the codes. Table 11 is therefore aligned with the findings as per Figure 4.

Due to the nature of the relationship between the codes within each environment, as represented by code links (see comments in lines joining two or more codes in Figure 4), further analysis was conducted. This analysis resulted in the consolidation and renaming of codes to best represent analytic findings gained from the interview process and from the grounded theory investigation of hypotheses 6 to 10.

The cumulative findings are presented in the next section as the final list of codes and families. This final list represents, what this thesis considers to be, the main artifacts and activities necessary to be performed by identified stakeholders in the digital forensic readiness process. This final step was also conducted using Atlas.ti, as described earlier.

**4.5.4 Development of final themes from code families and networks**

The final stage of the data analysis phase was to interpret code families and networks, in order to extrapolate key themes from each environment as discussed above. This process resulted in

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

the development of final themes and codes, which identify the three domains (derived from code families as previously discussed), from which key stakeholders in the digital forensic investigation originate. These include critical artifacts and activities, collectively referred to in this thesis as components (derived from codes from interviews and the analysis process) for each of the said domains. Finally, each code is assigned an abbreviation for ease of referencing.

**4.5.4.1 Components of the Corporate Environment**

From the review of findings relating to hypothesis 7, the deduction made is for organisations to establish a common standard for evidence handling, including associated procedures and policy. This in is line with the code *Corporate Culture* and its related findings as discussed in the preceding section.

Additionally, as deduced from hypothesis 6 in relation to the organisation, employees within the organisation are to be educated, trained and certified to properly prevent and detect digital crimes within the organisation. In this way employees will make themselves, and their organisations, less of a target for criminals. This is in line with the code *Industry targets* as discussed in the preceding section.

Finally, the deduction made from hypothesis 10 is that organisations need to be proactive (thus adopt digital forensic readiness) in managing the rising scourge of digital crimes. Focusing on digital forensic readiness addresses challenges noted in the preceding section relating to the codes: risks, prevalence of crime and industry targets. Table 12 summarises the transition from preliminary codes to final codes, as used in this study.

<b>Corporate Environment</b>		
<b>Preliminary Codes</b>	<b>Analysis</b>	<b>Final Codes</b>
Corporate Culture and Reporting	<i>Managed by enforcing Standards, Policies and Procedures</i>	Standards, Policies, Procedures
Risks	<i>Managed by empowered Human Resources</i>	Human Resources (ETC)
Prevalence of crime, Common crime and Industry targets	<i>Managed by proactive use of Digitally Forensic Ready Technologies</i>	DFR Technologies

Table 12: Corporate Environment - transition from preliminary to final codes.

The next section discusses the analysis of codes relating to the Industry Environment.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**4.5.4.2 Components of the Industry Environment**

Derived from the results of hypothesis 6, in order to avoid the risk of rendering evidence inadmissible, it is necessary that those individuals processing evidence possess the necessary knowledge and credentials to apply the digital forensic methodology. This is in line with codes, as discussed in the preceding section under Industry Environment. Finally, the final list of codes relating to this domain are derived from the adopted definition of digital forensics. These final codes represent activities associated with the digital forensic methodology and were found to be comprehensive enough in addressing challenges identified during the analysis of interview data relating to this domain and hypothesis 6. Table 13 summarises the transition from preliminary codes to the final codes as used in this study.

<b>Industry Environment</b>		
<b>Preliminary Codes</b>	<b>Analysis</b>	<b>Final Codes</b>
Knowledge	<i>Knowledge relating to all key phases of the digital forensic methodology, derived from Chapter 2, section 2.3</i>	Preservation
Credentials		Collection
Methodology		Validation
		Identification
		Analysis
		Interpretation
		Documentation
		Presentation
		Retention

Table 13: Industry Environment - transition from preliminary to final codes.

**4.5.4.3 Components of the Legislative Environment**

The preceding section identified legal culture, judiciary and eCrime law as codes that were noted during the analysis of interview data. The discussion of these codes point to challenges faced by this domain, in the prosecution of digital crimes. Combined with the results, as drawn from the discussion of hypothesis 6, findings show that the admissibility of electronic evidence is affected by factors which include: the presence of electronic laws, correct application of the criminal process by law enforcement and others during the investigation phase, a justice system that accommodates the nuances associated with digital crimes and justice personnel that are competent in prosecuting such crimes. Table 14 summarises the transition from preliminary codes to the final codes used in this study.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>Legislative Environment</b>		
<b>Preliminary Codes</b>	<b>Analysis</b>	<b>Final Codes</b>
Legal culture, Judiciary	<i>Willingness and ability to investigate/prosecute digital crimes</i>	Law Enforcement Agents, Justice Personnel
eCrime Law	<i>Establishment of specific laws relating to electronic evidence, in line with existing criminal processes.</i>	Criminal Process, Electronic Laws

Table 14: Industry Environment - transition from preliminary to final codes

The next section presents the consolidated final list of codes.

#### 4.5.4.4 Final literature themes

The final list of codes, as shown in Table 15, are discussed at length in Chapter 5 where a literature review is used as research method in an effort to gain a deeper understanding of their meaning and application in their respective domains.

<b>Corporate Environment (CE)</b>		<b>Industry Environment (IE)</b>		<b>Legislative Environment (LE)</b>	
<b>Ref</b>	<b>Component</b>	<b>Ref</b>	<b>Component</b>	<b>Ref</b>	<b>Component</b>
CE1	Standards	IE1	Preservation	LE1	Electronic Laws
CE2	Policies	IE2	Collection	LE2	Criminal Process
CE3	Procedures	IE3	Validation	LE3	Justice System
CE4	Human Resources (ETC)	IE4	Identification	LE4	Law Enforcement Agents
CE5	DFR Technologies	IE5	Analysis	LE5	Justice Personnel
		IE6	Interpretation		
		IE7	Documentation		
		IE8	Presentation		
		IE9	Retention		

Table 15: Final code themes developed from analysis of the interview data and literature relating to hypothesis 6 to 10.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**4.6 Triangulation of Findings**

Findings from this chapter were analysed in conjunction with those from the literature survey (Chapter 2) and a summary of the results is as per Table 16 below.

<b>Chapter 1 (Research Objective)</b>	<b>Chapter 2 (Literature review)</b>	<b>Chapter 4 (Interviews)</b>	<b>Triangulation Outcome</b>
RO1 - To identify common factors associated with technical and legal challenges faced in the prosecution of digital crimes.	H <sub>1</sub> - Electronic evidence gathered during a digital forensic investigation does not provide sufficient assurance of non-manipulation to the courts. = True	H <sub>6</sub> - As a result of the presence of the electronic laws in South Africa, the prosecution of digital crimes faces no limitations. = False	Findings show activities associated with ensuring <i>data integrity</i> to be a common technical challenge. The most common legal concern is the scope, or extent to which the law makes provision for the <i>admissibility</i> of electronic evidence in a court of law.
RO2 - To establish if organisations in the same legal jurisdiction possess, and make use of, a standard digital forensics methodology.	H <sub>2</sub> - There is a lack of standardisation in the criteria against which electronic evidence is validated as no consistent digital forensic methodology exists. = True	H <sub>7</sub> - South Africa has a standardised digital forensic model and process that is used by authorities to investigate and prosecute digital crimes. = False	Findings show that <i>no common standard</i> is used as a methodology, however, that organisations opt to develop internal methodologies from industry best practice guidelines.
RO3 - To determine the extent to which advances in digital forensics are meeting the demands of the changing legal and technical landscape.	H <sub>3</sub> - Forensic technology for gathering digital evidence is increasingly lagging behind the advances being made in anti-forensic tools and rapid changes in storage technology. = True	H <sub>8</sub> - The Electronic Communications and Transactions (ECT) Act of South Africa adequately positions the acceptable use of, and extent to which, electronic evidence can be used in a civil or criminal proceeding.	Findings suggest that digital forensics are <i>lagging</i> behind the rapid changes in <i>anti-forensics and storage technologies</i> . This is exasperated by the lack of <i>legal resources</i> and stakeholder <i>awareness</i> of DFR

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>Chapter 1 (Research Objective)</b>	<b>Chapter 2 (Literature review)</b>	<b>Chapter 4 (Interviews)</b>	<b>Triangulation Outcome</b>
		= True	principles.
RO4 - To investigate critical factors preventing human resources directly involved in the investigation and prosecution of digital crimes from functioning effectively.	H <sub>4</sub> - The people involved in the digital forensic investigation and prosecution process are not sufficiently trained and/or educated. = True	H <sub>9</sub> - Those involved in the prosecution of digital crimes are knowledgeable, adequately trained and professionally certified. = False	Findings show common limitations as being user <i>education, training and certification.</i>
RO5 - To determine if organisations are taking the necessary steps to proactively manage the rising scourge of digital crimes.	H <sub>5</sub> - An organisation responding to a digital crime without, an incident response plan, may take actions that compromise the admissibility of evidence to a court of law. = True	H <sub>10</sub> - South African organisations do not need to concern themselves with digital forensic readiness, as digital crimes are not commonplace. = False	Despite the growing trend of digital crimes against organisations across all industries, findings show a <i>general lack of digital forensic planning and readiness.</i>

Table 16: Summary of results from Chapters 2 and 4.

From the first research objective (RO1), this study found technical challenges to exist in activities associated with ensuring data integrity with the most common legal concern the scope, or extent, to which the law makes provision for the admissibility of electronic evidence in a court of law. This is an important finding as it directs efforts to specific data integrity issues which organisations need to be concerned with when undertaking a digital forensic investigation. For developing countries, this finding enforces the value that can be derived from extensively applying existing laws of evidence/common law, in the absence of laws specific to digital crimes.

Findings from the second research objectives (RO2) highlight the importance of the existence of industry best practice guidelines. Findings further show that countries which have not established and/or adopted a common digital forensic methodology, greatly benefit from

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

industry best practice guidelines.

The third research objective (RO3) speaks to the dynamic nature of the digital landscape. Findings suggest that digital forensics lag behind the rapid changes in anti-forensics and storage technologies. This situation is further exasperated by the lack of legal resources and stakeholder awareness of DRF principles. More importantly, these findings identify practical solutions that can be put into place at an organisational level, in order to address the identified gaps.

Findings from the fourth research objective (RO4) emphasise the importance of education, training and certification by human resources directly involved in the investigation and prosecution of digital crimes. This study also shows the detrimental effect which the lack of adequate education, training and certification can have on the admissibility of electronic evidence in the court of law, and the prosecution of cases involving digital evidence.

Finally, despite the challenges identified during the investigation of the preceding research objectives, findings from the fifth research objective (RO5) point to the critical nature of digital forensic planning and readiness as a proactive countermeasure to managing the rising scourge of digital crimes.

This study uses the above cumulative findings as a foundation to what the proposed model needs to address.

The next section presents the conclusion of this chapter.

### **4.7 Conclusion**

The goal of this chapter was to validate findings from the literature survey by making use of interviews as the key data gathering method. While the interviewee selection criteria appeared stringent, it attracted high calibre participants, representing multiple related disciplines.

The interpretive paradigm, applied with the assistance of Atlas.ti as the qualitative data analysis tool, provided a means to employ principles of immersion and crystallisation to the coded data. From this process, three families of themes (domains) emerged namely: Corporate Environment, Industry Environment and Legislative Environment. Additionally, this chapter presented key components which belong to each of the aforementioned domains, as detailed in Table 15.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

A summary of the results of the investigation into the validity of hypotheses 6 to 10 are:

- i. Hypothesis 6 (H6): Findings show that the hypothesis is not true. This suggests that a lack of processes, procedures, education, training and certification can serve as limitations during the prosecution of digital crimes.
- ii. Hypothesis 7: Findings show that the hypothesis is not true, as no single common model or process is in place for the South African legal context.
- iii. Hypothesis 8: Findings suggest that this hypothesis is true, as the ECT Act makes it possible to present electronic evidence in a court of law.
- iv. Hypothesis 9: Findings suggest that this hypothesis is not true, as credentials were noted as being a common limitation amongst prosecutors and investigations alike.
- v. Hypothesis 10: Findings suggest that this hypothesis is not true, as findings point to a prevalence of various types of digital crimes.

The next chapter presents the proposed conceptual model based on the above findings.



## **5. Chapter 5: Foundational principles towards model development**

---

### **5.1 Introduction**

The previous chapter focused on triangulating results from the systematic literature review (Chapter 2) and the interviews (Chapter 4). Findings presented confirmed, amongst others, that the three domains and their respective components, as shown in Table 15, are sufficiently inclusive for the purposes of this study.

This chapter is a continuation of Chapter 4, but with the goal of establishing the significance of each component of the model, as it relates to its respective domain. A further literature review is used to investigate the significance of each component. The components are discussed in the order in which they appear in Table 15.

This chapter concludes with a discussion on the multidimensional effect which each component of the model has.

### **5.2 Overview of the components of the proposed model**

This section provides depth and clarity to each component listed in Table 15.

#### **5.2.1 The Corporate Environment (CE)**

As previously discussed, the corporate environment refers to a code family (domain) that houses all identified components, which directly relate to activities and artifacts (components) that are under the control of the corporate, or organisation. These were identified as being standards, policies, procedures, human resources and digital forensic ready technologies. The next section uses a literature review to discuss the significance of these five components of the corporate environment.

##### **5.2.1.1 Standards (CE1)**

In its simplest sense, a standard is an agreed-upon way of doing something (Spivak et al., 2001) and, as such, it forms a cornerstone of the modern information economy (Greenstein et al., 2007). Standards are a means to create order and they denote a uniform set of measures,

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

agreements and conditions (Spivak et al., 2001; Grindley, 1995). In other words, standards act as a form of regulation.

Their use in the industry may be voluntary, or in some cases mandatory. Many standards are initially used voluntarily but over time they become adopted, or referenced, into mandatory regulations (Spivak et al., 2001). Egyedi et al. (2008) argue that when most people talk about standards, they usually refer to *de facto* standards. In economic terms, *de facto* standards are those that are widely adopted and with a significant market share (Bresnahan et al., 2007; Egyedi et al., 2008).

Greenstein et al. (2007) warn that standards affect firm strategy and market performance. Grindley (1995) adds that compatibility standards guide organisational strategy and policy, and affect overall business success. Therefore, it is vital that organisations be fully aware of industry standards and align their strategy and policies to those *de facto* standards that can adversely affect the organisation's competitiveness and compliance status.

The above suggests that standards form the foundation upon which policies and procedures are developed. As such they must be carefully researched to ensure that what the organisation or corporate finally creates, or adopts, is aligned to industry best practice (*de facto*) as it relates to the various aspects of digital forensic readiness.

### **5.2.1.2 Policies (CE2)**

Ben-Gera (2009) describes a policy as a “definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future actions.” Simply put, policies are guidelines that regulate organisational action (Campbell, 1998).

As mentioned in the preceding paragraph, organisational policies must be aligned to industry standards and organisational strategy. Peltier (2005) adds that to ensure that business objectives are met in a timely and efficient manner, effective policies and standards must be in place. As with standards, policies play a critical role in ensuring order in the way an organisation operates.

Page (2002) compares policies and procedures to a road map. At a glance, a map shows areas

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

of interest and the general direction in which to travel in order to reach a destination. The roads on the map are possible paths, or choices, one can take to reach a destination. Reaching a destination means that one needs to follow the correct roads. Similarly, a policy points out the general direction, or objective, to reach a certain destination or goal. On the other hand, a procedure provides the road or method to accomplish the objectives. It lays out steps to follow when performing repetitive work.

This suggests that policies can be an effective tool for organisations in that they document the correct path to travel, or actions to take, in the event of an incident.

The next paragraph further discusses the significance of organisational procedures.

### **5.2.1.3 Procedures (CE3)**

If policies are the organisational guidelines, procedures are the workhorses (Campbell, 1998). They are action-oriented and supplement the policy with specifics, thus completing the information that users need (Campbell, 1998; Page, 2002).

To fulfil their objectives, McConnel (2005) suggests that procedures (together with policies) should:

- i. Be clear, specific and provide adequate flexibility to meet changing conditions;
- ii. Comply with all appropriate laws and regulations and
- iii. Agree with one another and promote fairness and equality amongst employees.

Within the context of forensic readiness, organisational procedures provide a blueprint of how certain tasks are to be done, in the event of an incident. Additionally, procedures (coupled with policies) are a tool to manage employees. McConnel (2005) suggests that they serve numerous purposes, such as:

- i. Providing clear communication between the organisation and its employees;
- ii. Forming a basis for promoting fairness and equality;
- iii. Serving as guidelines for employees and management;
- iv. Serving as a basis for developing employee handbooks;
- v. Forming a basis for regular reviews of changes that affect employees and
- vi. Forming a context for employee training and orientation programmes.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Delaney et al. (1993) add that organisations must emphasise the management of employees (Human Resource Management), if they are to gain a competitive edge. He further states that modern, or progressive Human Resource Management policies and procedures, are positively associated with the economic performance of organisations.

The above suggests that the development of procedures is a forethought process that can help ensure that an organisation carefully considers and adopts actions that can serve to reduce the risk of inadvertently destroying and negating evidentiary data, whilst navigating the complex and multidisciplinary nature of digital crimes.

The next section discusses the significance of Human Resource Management.

### **5.2.1.4 Human Resources (CE4)**

Prince (2011) states that human resources encompass the people in an organisation (employees) and the human potential, or capital, available to a business. Human capital can be thought of as a stock of accumulated knowledge, skills and experience (Randhawa, 2007). It is a term that is increasingly used to refer to the philosophy, policies, procedures and practices related to the management of an organisation's employees (Wilson, 2005; Prince, 2011).

Human resource management (HRM) is concerned with all the activities that contribute to attracting, developing, motivating and maintaining a high performing workforce which results in organisational success (Randhawa, 2007).

Specific to the forensic readiness model presented in the last chapter, employee training and development were identified as critical components of the said model. Sims (2007) states that training and development, recently referred to as human resource development (HRD), consists of planned learning experiences that teach employees how to perform their jobs. It is concerned with orientation, performance management skills training and productivity enhancement. Randhawa (2007) adds that the objectives of HRD include:

- i. Training and developing staff to meet technological and social changes;
- ii. Ensuring a ready pool of competent staff at all levels to meet organisational needs at all times;
- iii. Preparing junior staff for future replacement;

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

- iv. Preventing staff obsolescence by inculcating new concepts in their areas and
- v. Promoting a high morale among employees.

Wilson (2005) argues that the proper management of HRD can improve organisational effectiveness and forensic readiness.

### **5.2.1.5 Digital Forensic Ready Technologies (CE5)**

Elliot et al. (2010) describe digital resilience as “the capability that an organisation develops to either withstand or recover from digital threats, and deal in an effective manner with the consequences of interruptions, failures or deliberate violation of digital systems.” Earlier in Chapter 2, the definition of digital forensic readiness was presented as the art of maximising the organisation’s ability to collect credible evidence, whilst minimising the impact to business operations whilst keeping investigative costs low.

Digital resilience and forensic readiness are concepts that are centred with the use of organisational data (Gladney, 2007). Franks (2012) argues that using organisational data appropriately will drive competitive advantage but he warns that ignoring organisational data will put an organisation at risk and cause it to fall behind the competition.

Therefore, the above suggests that organisations should use technologies that not only facilitate daily operational activities, but should also be concerned with protecting and preserving the integrity of organisational data, thereby increasing the organisational digital forensic readiness, or its ability withstand or recover from digital threats and incidents.

In addition to preserving organisational data for economic reasons, Runardotter et al. (2005) and Gladney (2007) argue that organisational data has to be available for future society for legal, historical and democratic reasons. The latter directly applies to this thesis as Chapter 3 was developed using case law which had been preserved and consequently benefited this study in the reaching of conclusions.

The next section discusses the significance of having investigative methodologies.

### **5.2.2 The Industry Environment (IE)**

The industry environment refers to a code family (domain) that houses all identified

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

components, which directly relate to activities and artifacts (domains) that relate to the forensic process of handling digital evidence. These components were previously identified as being: preservation, collection, validation, identification, analysis, interpretation, documentation and preservation.

The significance of each component of the digital forensic process is discussed next.

### **5.2.2.1 Preservation (IE1)**

Rice (2005) states that unless required by law, an entity is not obliged to preserve records. In addition, the duty to preserve evidence usually arises at the point when an incident has already occurred, or is suspected of having already occurred. However, this does not prevent an organisation from taking proactive measures in identifying critical information that can support an investigation in the event of an incident (Cooper et al., 2010).

Since electronic evidence may reside in numerous locations throughout an organisation's technological infrastructure, it is important to ensure that all possibly relevant sources for electronic data are identified (Nelson et al., 2006). These locations can include:

- i. Cloud Storage;
- ii. Servers and Mainframes;
- iii. Desktops and Laptops;
- iv. Mobile devices;
- v. Voice mail;
- vi. Printers and copiers;
- vii. Backup Media;
- viii. Removable and other portable storage devices and
- ix. Digital cameras and other multimedia devices.

Vacca (2005) warns that if the preservation stage is poorly implemented, it gives rise to numerous possibilities for error in the form of destruction, mishandling and contamination. Therefore, it is imperative that this step of the methodology be carried out with exactness to ensure that the integrity of the evidence is maintained.

Once evidence is preserved, the next step is to isolate it from the crime scene for purposes of analysis. This is discussed in the next step.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **5.2.2.2 Collection (IE2)**

Shavers (2013) argues that digital forensic investigations follow the same rules of evidence as any other investigation. Additionally, that digital evidence must be seized according to evidentiary procedures of the investigators agency and legal rules of evidence.

As discussed in Chapter 2, the acquisition of electronic evidence has different implications and objectives when compared to the method of seizure and preservation of non-physical evidence. Furthermore, based on the type of evidence, a common decision to make is whether the evidence should be collected using *live* or *dead* forensic techniques, as discussed in Chapter 2. Since each case is different, it is up to the investigator to decide which method is most reasonable when approaching the computer systems at the particular scene (Kizza, 2005; Shavers, 2013).

### **5.2.2.3 Validation (IE3)**

The objective in a digital forensic investigation is to present evidence in such a way that it can be used as evidence in a court of law (Vacca, 2005). This means that, unlike other computing areas where speed is the main concern, the priority in digital forensics is accuracy. To verify data integrity, methods such as the use algorithms are available (Nelson et al. 2010). In addition to using hashing algorithms, as discussed in Chapter 2, Vacca (2005) proposes the following four considerations to validating electronic evidence:

- i. Authenticity: establishing if electronic evidence comes from where it purports.
- ii. Reliability: establishing if there are any reasons for doubting the correct working of the computer.
- iii. Completeness: establishing if evidence obtained represents the complete picture.
- iv. Freedom from interference and contamination.

Only once the evidence is correctly validated can the investigator invest time to unpack the content of the digital evidence piece in question. The significance of this step is discussed next.

### **5.2.2.4 Identification (IE4)**

Nelson et al. (2010) state that in litigation cases, the investigator is often required to recover as much as possible, resulting in *scope creep*. They further warn that scope creep increases the time and resources needed to extract, analyse and present evidence. As discussed in Chapter

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

4, this situation may lead to the discovery of evidence that is out of scope, which may harm the admissibility of evidence and credibility of the investigator (Hypothesis 1, Chapter 4).

Once the identification of evidence that falls within the parameters defined by the scope has taken place, analysis may begin.

### **5.2.2.5 Analysis (IE5)**

During this step, it is important to understand the chronology of events and to link together key artifacts in order to understand the complete picture. Making use of the correct forensic technology will not only expedite the analysis phase, it will also create a safety net that ensures and confirms that the investigator did indeed operate within the parameters set by the investigation scope. Daniel et al. (2012) propose that the following be considered when using technology for forensic analysis. For a tool to be forensically sound, it must be:

- i. **Definable:** enable the investigator to state the problem, articulate the desired outcome, develop an algorithm to describe the process and have a measurement system to validate the process;
- ii. **Predictable:** the tool must be predictable. If it is used to find pictures of certain format, then the prediction is that it will always find those types of files and
- iii. **Verifiable:** the ability to verify results and arrive at the same conclusion.

The output of the tool must be interpreted to establish its relevance to the investigation (Daniel et al., 2012). Interpretation is discussed next.

### **5.2.2.6 Interpretation (IE6)**

The interpretation step is concerned with contextualising the results of the analysis phase in a way that demonstrates the logical flow of events. It is during this step of the methodology that the true value of a forensic expert is realised. Daniel et al. (2012) argue that failing to make a decision to hire an expert early in the process can lead to sanctions, or inadmissibility, of evidence critical to a case.

As discussed in Chapter 4, an error in interpretation by the expert witness may harm the admissibility of evidence, and tarnish the expert's credibility (Hypothesis 1, Chapter 4).



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **5.2.2.7 Documentation (IE7)**

This step entails the documentation and presentation of findings in an appropriate manner. The examiner's final report is a document which is delivered to the prosecutors, opposing counsel and other relevant parties, towards the end of the investigation. Sammons (2012) suggests that this document typically consists of:

- i. The identity of the reporting agency;
- ii. A case identification reference number;
- iii. Identity of the submitting person, including the case number;
- iv. Dates of the receipt and report;
- v. Detailed description of the evidence items submitted;
- vi. Identity of the examiner;
- vii. Description of the steps taken during the examination process and
- viii. Detailed findings and conclusions.

The aim of this step is to provide the reader with a document that is understandable and accurately represents the forensic process followed (Daniel et al., 2012).

### **5.2.2.8 Presentation (IE8)**

Following the presentation of results in a report, the next necessary step is to preserve the evidence for a period as determined by the law. With digital evidence, it is up to the investigator to consider how and on what type of media to store it and what storage media is best to secure it (Nelson et al., 2010). Additionally, the decision regarding the storage media used will also be determined by how long the evidence needs to be stored for. This means it is important that the correct media is used in order to prevent the risk of device obsolescence.

It is important to remember that all records, whether electronic or not, should be retained for at least the minimum period stated in any applicable statute or regulation (Francis, 2004; Nelson et al., 2006).

Specific to the South African law, the Criminal Procedure Act (Lawlibrary, n.d) stipulates that "the judge or judicial officer presiding at criminal proceedings shall at the conclusion of such proceedings, but subject to the provisions of this Act or any other law under which any matter shall or may be forfeited, make an order that any article referred to in section 33" and offers the following conditions for the disposal of articles after commencement of criminal

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

proceedings:

- i. That the article be returned to the person from whom it was seized, if such person may lawfully possess such article;
- ii. If such person is not entitled to the article or cannot lawfully possess the article, be returned to any other person entitled thereto, if such person may lawfully possess the article or
- iii. If no person is entitled to the article or if no person may lawfully possess the article or, if the person who is entitled thereto cannot be traced or is unknown, be forfeited to the State.

Therefore, it is of the utmost importance that organisational policy and legal requirements be considered when dealing with the destruction or disposal of assets, articles or evidence that is no longer needed for preservation and retention (Nelson et al., 2006).

The next section discusses the significance of the components found in the legislative environment.

### **5.2.3 The Legislative Environment (LE)**

As INTERPOL Secretary General Ronald K. Noble once commented, “global efforts against cybercrime and to enhance cyber security require law enforcement and private sector Internet security companies to work more closely together, as well as harmonised regulations across countries” (Interpol, 2013).

This notion supports the theme of this study namely that forensic readiness can only be achieved through cooperation and collaboration between parties from varying domains, as shown in Table 15.

The legislative environment refers to a code family (domain) that houses all identified components, which directly relate to activities and artifacts (domains) that relate to the judicial system in the prosecution of digital crimes. These components were previously identified as being: electronic laws, criminal process, justice system, law enforcement agents and justice personnel.

The next section discusses the significance of the judicial system in the forensic readiness

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

process.

### **5.2.3.1 Electronic Laws (LE1)**

As discussed in Chapter 4, traditional laws were not developed with the cyber society in mind. Shalhoub et al. (2010) argue that while a number of countries around the world have reformed their existing laws and legislation to cater for digital crimes, this has provided vague and inefficient solutions. Additionally, that for ethical standards to be established in cyber space, new laws have to be legislated to deal with cybercrimes.

Mambi (2010) proposes the following paradoxes for consideration when developing electronic laws:

- i. Such laws must include almost all branches of law. However, in order to be meaningful, it must be narrowed down and delimited;
- ii. Electronic laws must include be technologically neutral, but be able to steer and regulate technology and its various uses;
- iii. The development of electronic laws requires broad, as well as deep understanding of machinery and methods. However, legal solutions must be simple to understand and apply and
- iv. Such laws require foresight. However, it is difficult to predict future developments, situations, applications and issues in the technology sector.

The above points suggest that, while traditional laws may serve to facilitate the admissibility of electronic evidence in a court of law, such attempts are inefficient solutions. This dilemma can be resolved by legislating new laws that specifically deal with cybercrimes.

### **5.2.3.2 Criminal Process (LE2)**

Chapter 4 presented a discussion which supports the view that digital evidence is collected differently than eyewitness testimony or physical evidence, and as such, a proposed that a process was required to address digital evidence.

The criminal procedure under the traditional law has evolved to regulate the mechanisms common to the investigation of physical crime, namely the collection of physical evidence and eyewitness testimony. Kerr (2005) warns that digital evidence will trigger new rules of

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

criminal procedure simply because computer related crimes feature new facts, and that these facts demand new laws. To that, Krige (2012) added that electronic evidence still needs to pass the legal scrutiny of relevance and authenticity.

This suggests that while it is possible to prosecute digital crimes under the traditional laws and processes (see Hypothesis 11, Chapter 4), technological advances continue to introduce limitations that make it necessary to not only develop electronic laws, but to ensure that complimentary criminal processes exist.

These processes will enable law enforcement to conduct their investigations in a forensically sound manner.

### **5.2.3.3 Law Enforcement Agents (LE3)**

As discussed in Chapter 2, education, training and awareness of law enforcement agents and justice personnel is necessary to enable them to attain the competencies required to effectively deal with digital crimes (Hypothesis 4, Chapter 2).

Digital forensic experts specifically need to obtain certification in the tools and techniques used during the digital forensic process. Schlichting et al. (2004) explained that certification involves the extensive testing of a person's abilities in his/her area of specialisation.

Finally, while awareness can be achieved during the education, training or certification process, its goal is simply to change one's sensitivity towards a given topic or issue (Rogers et al., 2004; Cross, 2006).

Rogers et al. (2004) stated that education, training and certification were the most reported inherent challenges facing digital forensic practitioners and law enforcement alike. Hoolachan et al. (2010) added that the problem is compounded by the lack of a standardised, or consensus, approach to training computer forensics practitioners which can negatively impact on an organisation's Forensic Readiness.

The above points to a need for law enforcement and digital forensic practitioners to be frequently exposed to the necessary opportunities to develop and maintain their skills through various education, training and awareness programmes.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **5.2.3.4 Justice Personnel (LE4)**

The findings in Chapter 4 show that the judiciary is presented with two problems that result in a reluctance to prioritise on digital evidence: high caseloads and a lack of knowledge (see Chapter 4, section 4.4.6, Question 13).

Efforts, such as the United States Department of Justice hosting a conference on this subject (The US Department of Justice, 2009), create interest in dealing with digital crimes, but also aid in encouraging international cooperation. This can contribute to addressing the lack of knowledge problem.

Furthermore, this is a challenge that many organisations face and it requires organisational commitment to invest in empowering staff with knowledge and tools in order to perform their duties (see Hypothesis 4, Chapter 2).

Lienhard et al. (2011) argue that in most countries of the world the judiciary experience increasing workloads, while scarcely any additional resources are available to cope with the problem. They propose that a truly effective system of court management could address the problem. This suggests that the high caseload is a systemic problem and requires looking at the system.

### **5.2.3.5 Justice System (LE5)**

Chapter 4 identified high caseloads and a lack of knowledge as the two factors contributing to inefficiencies when prosecuting digital crimes. The topic of knowledge was addressed earlier in this chapter. In addition, respondents interviewed indicated that one of the possible solutions to addressing high caseloads was the development of special cybercrime courts. This suggestion was found to be in harmony with studies conducted by Fox et al. (2013). In this study, Fox et al. (2013) identify the following as measures for improving case processing in the courts of law:

- i. Flexible court sittings, including early morning, evening and weekend sittings for certain types of hearings;
- ii. Reducing the number of continuances;
- iii. Setting time limits on case processing for detainees;
- iv. Cooperation and collaboration between judges, prosecutors, defence attorneys and law enforcement and
- v. Fast tracking cases where a guilty plea is anticipated.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

As discussed in Chapter 4, advances in the judicial system are required to ensure robustness, maturity and effectiveness in dealing with digital crimes. The latter is a view shared by United Nations Secretary-General Ban Ki-moon who stated that “we cannot expect to gain our goals of peace, development and respect for human rights without promoting and supporting a robust system of international criminal justice. That is our shared responsibility. It is our common interest” (United Nations Radio, 2013).

The above discussion serves to provide the context and meaning behind the components as listed in Table 15. Figure 4 is a graphic representation which seeks to provide both a summary of the above discussion and a foundation upon which the proposed model will be built.

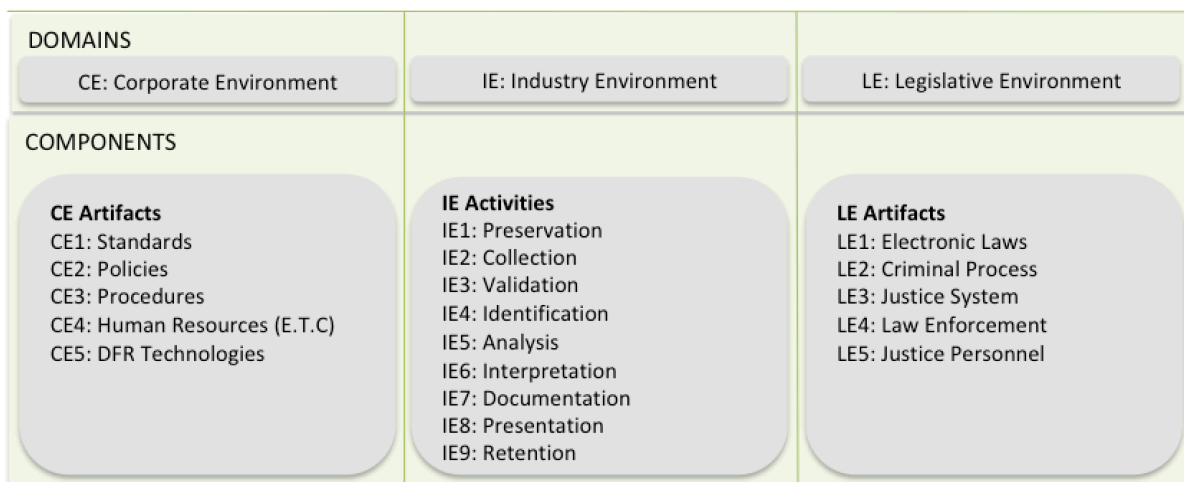


Figure 5: Building blocks for the proposed model.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**5.2.4 The Multidimensional Effect**

Analysis of the literature suggests that the components and domains discussed in this chapter, have a multidimensional effect. At an application level, it is therefore necessary to establish the *locality* of each component, preceded by considerations on interdependencies that may exist. As per Table 17, findings suggest that when determining the locality of each component, the following three categories and their respective definitions serve as guidelines:

- i. Local Component: A component whose attributes are unique to a single entity (company and/or country) and whose scope is limited to its immediate environment.
- ii. Global Component: A component whose attributes are common across multiple entities (countries), and whose scope is not limited to its immediate environment.
- iii. Hybrid Component: A component possessing attributes of mixed origins (Local and Global) and whose scope satisfies (in part or in full) its immediate and broader environments. This component is characterised by customisation, with emphasis on either the local or global scope.

Corporate Environment			Industry Environment			Legislative Environment		
Ref	Component	Locality	Ref	Component	Locality	Ref	Component	Locality
CE1	Standards	Hybrid	IE1	Preservation	Global	LE1	Electronic Laws	Hybrid
CE2	Policies	Local	IE2	Collection	Global	LE2	Criminal Process	Hybrid
CE3	Procedures	Local	IE3	Validation	Global	LE3	Justice System	Hybrid
CE4	Human Resources (ETC)	Local	IE4	Identification	Global	LE4	Law Enforcement Agents	Local
CE5	DFR Technologies	Hybrid	IE5	Analysis	Global	LE5	Justice Personnel	Local
			IE6	Interpretation	Global			
			IE7	Documentation	Global			
			IE8	Presentation	Global			

Table 17: Characterisation of components.

**5.2.4.1 Local Components**

As shown in Table 17, local components exist in both the Corporate Environment (CE) and the Legislative Environment (LE). While local in scope, the foundations (CE1, LE1, LE2 and LE3)

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

of these components contain attributes of mixed origins. This interdependency suggests that while local components have limited scope, their attributes must not be isolated from the global environment but must be expandable and in harmony with the surrounding environments (*customisation* and *adaptation*). However, the expandability and harmonisation of local components to the global environment is not a one-way process, as discussed in the next paragraph.

### **5.2.4.2 Global Components**

Global components only exist in the Industry Environment (IE). This suggests that while a digital forensic methodology can be localised, its design principles remain largely governed by global/international best practices. Furthermore, findings suggest that while localisation can take place at a granular level, the guiding global principles remains. This localisation of global components creates a two-way process that facilitates harmony between local and global components.

### **5.2.4.3 Hybrid Components**

As depicted in Table 17, hybrid components exist in both the Corporate Environment (CE) and the Legislative Environment (LE). An analysis of these components shows that they are largely foundational in nature, and form the basis from which the attributes of local components are derived. Hybrid components are testament to the interdependencies that exist between local and global components.

### **5.2.4.4 Conflict Management**

In a perfect system, all components work in harmony, without any conflict. However, literature review findings suggest that this may not always be the case. The challenge is to create harmony between the corporate, industry and legislative environment thereby increasing the probability of the admissibility of electronic evidence in a court of law.

It is with the above in mind that the assumption that conflicts between the local, global and hybrid components will exist, is made. In such a situation, careful consideration must be applied to establishing the source and nature of the conflict, whilst giving priority to the laws of the land, followed by industry regulations and finally organisational needs.

The next section discusses how this information on domains, and their respective components,



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

was used in developing the M-DiFoRe model.

### **5.3 The Conceptual Modelling Process**

As Verdonck (2014) explained, conceptual modelling is an activity concerned with representing aspects of the physical and social world for communication, learning and problem solving among human users. Hoppenbrouwers (2005) added that in conceptual modelling, the fundamental assumption is that viewers perceive a universe and then produce a conception of that part which they hold as relevant. Furthermore, that the conceptions harboured by a viewer cannot be communicated and discussed with other viewers unless they are articulated in some form. In other words, a conception needs to be represented.

The conceptual modelling process was found to align with the research approach (post modernism) adopted in this study, as discussed in section 1.7. As already noted, the post modernism approach assumes a philosophical position which proposes that reality is constructed within belief systems, and that the observer is an integral part in what is being observed. The adopted conceptual modelling process provided a practical way of communicating the *reality* under investigation by presenting it in a demystified and simplified manner towards solving the *problems* investigated in this study.

#### **5.3.1 Procedural Guidelines**

Verdonck (2014) opined that the quality of conceptual models can be improved by applying a defined conceptual modelling process. The following six steps to conceptual modelling are proposed:

- i. Step 1: Recognising the need for a conceptual model. A conceptual model must be developed for the purposes of communication, learning and problem solving. A conceptual model must seek to answer a specific question, or set of questions.
- ii. Step 2: Determining the modelling strategy. The general guidelines for this step is that the modelling strategy should accompany the modeller throughout the path of developing a conceptual model. Such a strategy serves to retain the modeller from making sudden changes or modifications during the modelling process, which could lead to a lower quality conceptual model.
- iii. Step 3: Conception of the conceptual model. This requires the modeller to form a first conception of the model. During the formation of a conception, the modeller identifies the main objects of the real world that need to be modelled. In other words, a blueprint

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

of the conceptual model is created, where the main objects and their relationships or dependencies are identified.

- iv. Step 4: Choice of an ontology. Ontologies can be used as a basis for a modeller's perception of the real world, which will have an impact on the actual modelling of the real world. The ontology will give the modeller a perception of the real world, which can then be used to correctly create a representation of the real world.
- v. Step 5: Choice of a conceptual modelling language. The choice of the conceptual modelling language depends on the modelling strategy and the preferred ontology. Conceptual modelling is deeply rooted in communication, involving language as a means to achieve communication.
- vi. Step 6: Realisation of the conceptual model: As a final step, the conceptual model can be created to represent the chosen aspect of the real world. The developed model should fulfil two sets of demands on quality, one related to verifiability (i.e. internal quality) of a model and the other related to validity (i.e. external quality) of a model.

By formulating, and applying, a modelling strategy as part of the conceptual modelling process and carefully linking the modelling needs/requirements to a certain ontology and conceptual modelling language, the developed conceptual model will result into a valid model, achieving both verification and validation (Grady, 1998; Unhelkar, 2005; Verdonck, 2014).

### **5.3.2 Applied Modelling Process**

In developing the M-DiFoRe model, this thesis applied the above mentioned steps, as follows:

- i. Step 1: Recognising the need for a conceptual model. Chapter 1 of this thesis sets out the problem statement (section 1.3), research objectives (section 1.4) and its accompanying hypotheses (section 1.5) and proposes the development of a model to solve the identified problem/need.
- ii. Step 2: Determining the modelling strategy. As applied in Chapters 6 and 7, the strategy adopted in developing the M-DiFoRe model was to:
  - a. Review literature in the form of case law, as documented by the South African courts. The cases selected meet a specific criterion, as described in Chapter 6, section 6.2.1.
  - b. Analyse the literature using Atlas.ti, following the process as detailed in Chapter 4.
  - c. Interpret results of the analysis process and establish the existence and nature of

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

the interdependencies that exist in the codes and families (domains and components) as per Chapter 4, Table 15.

- d. Develop the model using an integrated testing approach, in which verification and validation take place throughout the development process, and not at the end of the model development phase (Cook et al., 2005; Debbabi et al., 2010; Verdonck, 2014).
- iii. Step 3: Conception of the conceptual model. This thesis identified the blueprint, or main objects of the real world that need to be modelled as those contained in Table 15. Table 15 lists the main objects (domains and components), whose inter-dependencies are investigated as part of model development and testing (Chapters 6 and 7).
- iv. Step 4: Choice of an ontology. The ontology adopted in this study is presented in Chapter 3. In order to meet the ontological quality requirements for completeness, accuracy and cognitive adequacy, an iterative process was followed in reviewing and coding selected case law, until theoretical saturation was reached. The latter is discussed in section 6.2.1.
- v. Step 5: Choice of a conceptual modelling language. The M-DiFoRe model is developed using the Natural Conceptual Modelling Language (NCML), focusing on the primary syntactic elements of natural language, namely: nouns, verbs and the prepositions associated with verbs (Boyd, 1998). In line with NCML guidelines provided by Boyd (1998), this thesis shows the elements of NCML as rectangles, labelled arrows and lines. Labelled rectangles represent sentence subjects and objects, while labelled arrows represent verbs and labelled lines represent prepositions that contribute to the predicates of the verbs. Chapter 6, Table 18, contains a summary of the arrows and lines used in this thesis, and their respective meanings.
- vi. Step 6: Realisation of the conceptual model: The representation and explanation of the M-DiFoRe model is documented in Chapter 6, sections 6.3 and 6.4. In order to meet quality demands, verification and validation activities can occur throughout the model development phase in addition to, and/or as an alternative approach to testing post development (Cook et al., 2005; Debbabi et al., 2010; Verdonck, 2014). This thesis presents the application of the abovementioned Steps 5 and 6, which detail the model development process and continuous verification in Chapter 6, followed by the validation of the M-DiFoRe model in Chapter 7.

## **5.4 Conclusion**

This chapter presented a continuation of Chapter 4, but with the goal of establishing the significance of each component of the model, as it relates to its respective domain.

A literature review was used to investigate the significance of each component. Table 15 was used as a basis for the literature review presented in this chapter. Findings serve to provide a theoretical foundation for the development of the proposed model presented in Chapter 6. This was followed by a discussion on the multidimensional effect of each component under the three domains, as shown in Table 17.

Finally, this chapter concludes with a presentation of the literature relating to the conceptual modelling process and details how this process was applied towards developing the M-DiFoRe model.

The next chapter presents the application of the model development and testing process, as described in section 5.3.2.

## **6. Chapter 6: Realisation of the Conceptual Model**

---

### **6.1 Introduction**

The work presented in this chapter builds on the theoretical foundation formed in Chapter 5, which comprises a blueprint of the conceptual model wherein the main objects and their relationships are identified.

This chapter is concerned with the realisation of the conceptual model which, as Verdonck (2014) explained, is the final step in applying the conceptual modelling process. The application of Verdonck's (2014) conceptual modelling process in this chapter is detailed in section 5.3.2. The goal is to develop the conceptual model through the investigation of the interdependencies that exist between the components from the three domains (Table 15), as discussed in the previous chapter.

In addition to this chapter describing the realisation or development of the model, it will also verify the accuracy and completeness of the blueprint (Table 15) which identifies the domains and their respective components. This is achieved by following the modelling strategy, as detailed in section 5.3.2. This integrated approach was undertaken to build confidence and credibility in the blueprint (Thacker et al., 2004).

Thacker et al. (2004) state that both *verification* and *validation* are processes that accumulate evidence of a model's correctness or accuracy for a specific scenario; thus, the two processes cannot prove that a model is correct and accurate for all possible scenarios, but rather that the model is sufficiently accurate for its intended use. The verification of the model is presented in this chapter while the validation process is presented in Chapter 7.

As per section 5.3.2, Step 2(a), the work presented in this chapter stems from an analysis of case law as presented in the South African courts, wherein electronic evidence formed a key part of evidence led during legal proceedings. This chapter presents the three cases and analyses them against critical components and domains, as discussed in the previous chapter (Table 15). The results of this analysis are used to identify the interdependencies between the three domains and their respective components, the results of which are then used to develop the conceptual model.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

This chapter concludes with a discussion on *how* the proposed model can be used to enable organisations to reduce the potential dangers from the inadvertent destruction and negating of evidentiary data, and to so improve overall organisational digital forensic readiness. In addition, this chapter presents a template against which a *self-assessment* can be conducted, when applying the model within an organisation.

### **6.2 Model Development Protocol**

This section presents an analysis of case law to verify components of the proposed model. After following the protocol presented hereafter, findings started showing the same results after the third case that was analysed. With theoretical saturation reached (Vogt et al., 2014; Beaudry et al., 2016), detailed analysis was only limited to the 3 case law presented in the sections that follow.

#### **6.2.1 Scoping and Database Section**

The scope of our research was limited to material available on the Southern African Legal Information Institute (SAFLII, 2016) online database which publishes legal information for free public access. It mainly comprises case law and legislation from the South African High Court.

A detailed search of relevant databases was conducted. The criteria for relevance was based on the following factors:

- i. Case law from South African courts only: This is particularly important as the legal context for this research is limited to South African law, as described in Chapters 2 and 3, respectively.
- ii. Case law post 2002, after implementation of the ECT Act: This is keeping in line with the legal context described in Chapter 2, section 2.3.
- iii. Case must be transcribed in English: This in keeping with the scoping criteria described in Chapter 2, section 2.3.
- iv. Electronic evidence must form part of key evidence led: The analysis phase can thus discover important aspects of the case which led to the admissibility, or inadmissibility, of electronic evidence presented.

This analysis made use of the same keywords as presented in section 2.2, which were also used in the literature review.

The last step was to analyse each case law to test if it matches the last criteria, which requires

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

that electronic evidence must form part of key evidence led. From this exercise, three cases were selected for further detailed analysis using the Atlas.ti tool (Atlas.ti, 2012). This yielded a collective total of seven cases for review. The research was limited to three cases as theoretical saturation of data was reached by the third case, and findings from the analysis of each case yielded similar results (Vogt et al., 2014; Beaudry et al., 2016). This negated the justification for sampling of additional cases.

The next sections present the three cases and their respective synopsis.

### **6.2.2 Selected Case Law**

The three cases selected refer to:

- i. Cellular Telephone Records (SAFLII, 2008),
- ii. Computer and Network data (SAFLII, 2014[a]) and
- iii. Customer Banking Records (SAFLII, 2014[b]).

All the above cases are in the public domain and thus meet the University of South Africa's policy on research ethics, as discussed in Chapter 1.

The next section presents the merits of the court case in question.

## **6.3 Findings**

This section provides a synopsis to the three cases analysed in this chapter as well as demonstrate the interdependencies that exist between the components from the three domains.

### **6.3.1 Case Law Synopses**

The full case files, along with the coded and analysed Atlas.ti (Atlas.ti, 2012) relational diagrams (data maps) are attached as Appendices 5, 6 and 7, respectively.

#### **6.3.1.1 Cellular Telephone Records**

The first case took place in June 2003 and involved trucks carrying a large consignment of cigarettes belonging to The British American Tobacco Company of South Africa (BATSA),

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

which was hijacked by armed robbers. This happened three times. In all three incidents the contents of the truck was loaded onto another truck whilst the BATSA driver and his assistant were removed from the scene and later released, unharmed.

In each case, the modus operandi used to stop the BATSA truck was a replica police vehicle equipped with a flashing blue light and driven by persons wearing police, or traffic officer, uniforms. After flagging down the BATSA truck and making some initial enquiry relating to the driver's licence, or the cargo being carried, the criminals produced firearms and held up the driver and his assistant.

The chief pillar of the State's case was the evidence of the S204 accomplice witness, Vernon Aspeling. The second pillar consisted of the records of the cell phone activity of various cell phones allegedly used by, inter alia, accused 1, 2, 3, 4, 6, 7 and 8. Through this evidence the State sought to demonstrate that the accused were present at the scenes of one, or more, of the three robberies and were in contact with each other before, during and after such robberies (SAFLII, 2008). See Appendix 5 for the full case, coded data and Atlas.ti relational diagrams.

### **6.3.1.2 Computer and Network Data**

The second case relates to defamatory and injurious allegations sent to customers concerning Bytes Managed Services (Bytes MS) by a disgruntled ex-employee of Bytes MS. In these emails the defendant alleges that, while employed by Bytes MS, he was involved in an internal investigation sanctioned by himself and conducted with the assistance of 15 other employees to determine whether there were irregularities in the service delivery from Bytes MS to its customers. He also informed the recipients that the matter had escalated to the level of enquiry by the National Prosecuting Authority and the Competition Commission.

The defendant was employed by Bytes MS as a Business Development Executive from 2007 to 2009. Owing to the scope and type of confidential and sensitive documentation and information which the Defendant was privy to, he was required to sign various confidentiality undertakings. The Defendant was dismissed in February 2009 due to insubordination and irretrievable breakdown of the trust relationship. The Defendant's dismissal resulted from his failure to follow frequently repeated and clear (written and oral) instructions in relation to a certain transaction which resulted in a bad debt provision of R3.2 million, one month prior to the financial year end of the First Plaintiff.



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

The case was based on an analysis of electronic copies of various emails in which the author used the alias “Sunita Paritala”. These emails contained defamatory and injurious allegations. The court required digital forensic experts to trace the emails and establish their origin, analyse all emails received from the Defendant, his legal representative and “Sunita Paritala” and to establish if the Defendant was involved in distributing these emails, either by supplying the information to, or posing as, “Sunita Paritala” (SAFLII, 2016[a]).

See Appendix 6 for the full case, coded data and Atlas.ti relational diagrams.

### **6.3.1.3 Customer Banking Records**

The last case involves the use of stolen login details of Postbank customers. The suspects were arrested after the discovery of a syndicate, the members of which allegedly stole R2 million from bank accounts, held by the public, at various Post Office outlets.

The theft occurred in 2011 and the suspects were linked to another similar theft which had occurred in 2008. With the assistance of Post Office employees, the suspects had obtained details of Post Office banking accounts into which vast amounts of money had been deposited, and were being held. Identity documents, passports and other documents were falsified in order to access and divert the funds deposited in these bank accounts. Thereafter, the funds held in said bank accounts were unlawfully depleted through the connivance of members of the syndicate, who had formerly been in the employ of the Post Office.

Details of some of the targeted bank accounts (including references to the Post Office bank account numbers, balances, account holders’ names and contact details) were allegedly discovered stored on the suspects’ cell phones (SAFLII, 2014[c]).

The State’s case was based on an analysis of computers, cellular phone data and other security logs, which were then used to reconstruct the scene and link the criminal activities to the suspected individuals.

See Appendix 7 for the full case, coded data and Atlas.ti relational diagrams.

### **6.3.2 Process for Data Coding**

The coding, mapping and analysis of case law data followed the same approach as discussed

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

in Chapter 4, which discusses the development of codes, families and networks. Table 15, shows the common set of codes which was developed during the analysis of interview data and is used in this chapter as a foundation towards the validation of the three cases.

Results from the analysis of the three cases, using the keywords in Table 15, show that all codes were found to exist in all three cases and that no new codes had emerged during the analysis process. The study therefore accepts Table 15 as a final list of codes from which further analysis will take place. The consistency in findings between Chapters 2, 4 and 6 further acts as confirmation that the triangulation process was successful.

Once codes were formed, they were further correlated into one to identify shared conceptual characteristics. This was necessary in order to understand the relationship and interdependencies between the codes. Where codes were found to relate to each other, memos were created to narrate the nature of their relationship. Additionally, linkages were formed using either a black line (to represent a link which led to evidence being admitted in court) or a black line (to represent an action the court deemed detrimental to the case).

Five types of linkage lines were used, each serving a specific purpose. The linkage lines also had arrows to depict the flow of information. Both bi-directional and uni-directional arrows were used. Table 18 summarises the meaning of each link type and its associated arrow.

From the above analysis, groupings of codes sharing conceptual characteristics emerged. The code groupings, or code families, were analysed further and given family names, based on their collective function.

<b>Link type</b>	<b>Link type reference</b>	<b>Arrow type</b>	<b>Arrow type reference</b>	<b>Synopsis</b>
Comply with	Co	Uni-directional arrow	Uni-D	Act in accordance with set law or policy.
Cooperate with	Coo	Uni-directional arrow	Uni-D	Act jointly or assist with an action.
Is a property of	Pr	Uni-directional arrow	Uni-D	Belongs to, or is a subset of.
Must achieve	Ac	Uni-directional arrow	Uni-D	A required output or action.
Is associated with	As	Bi-directional arrow	Bi-D	Sharing a common purpose.

Table 18: Link and arrow types used to investigate relationships between components.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Finally, Atlas.ti was used to graphically represent the interdependencies between the codes, making use of different link and arrow types, as previously discussed. This process is represented in Figure 6.

The next section discusses the code families that were formed, and presents the function of each code family.

### **6.3.3 Mapping of Code Families**

From the analysis of the code families, and component interdependency chart presented in Figure 6, findings show the following systems, or groupings of components based on a function they perform:

- i. Group 1: These are systems with two components from different domains;
- ii. Group 2: These components form systems with three components, and
- iii. Group 3: These components form systems with more than three components.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

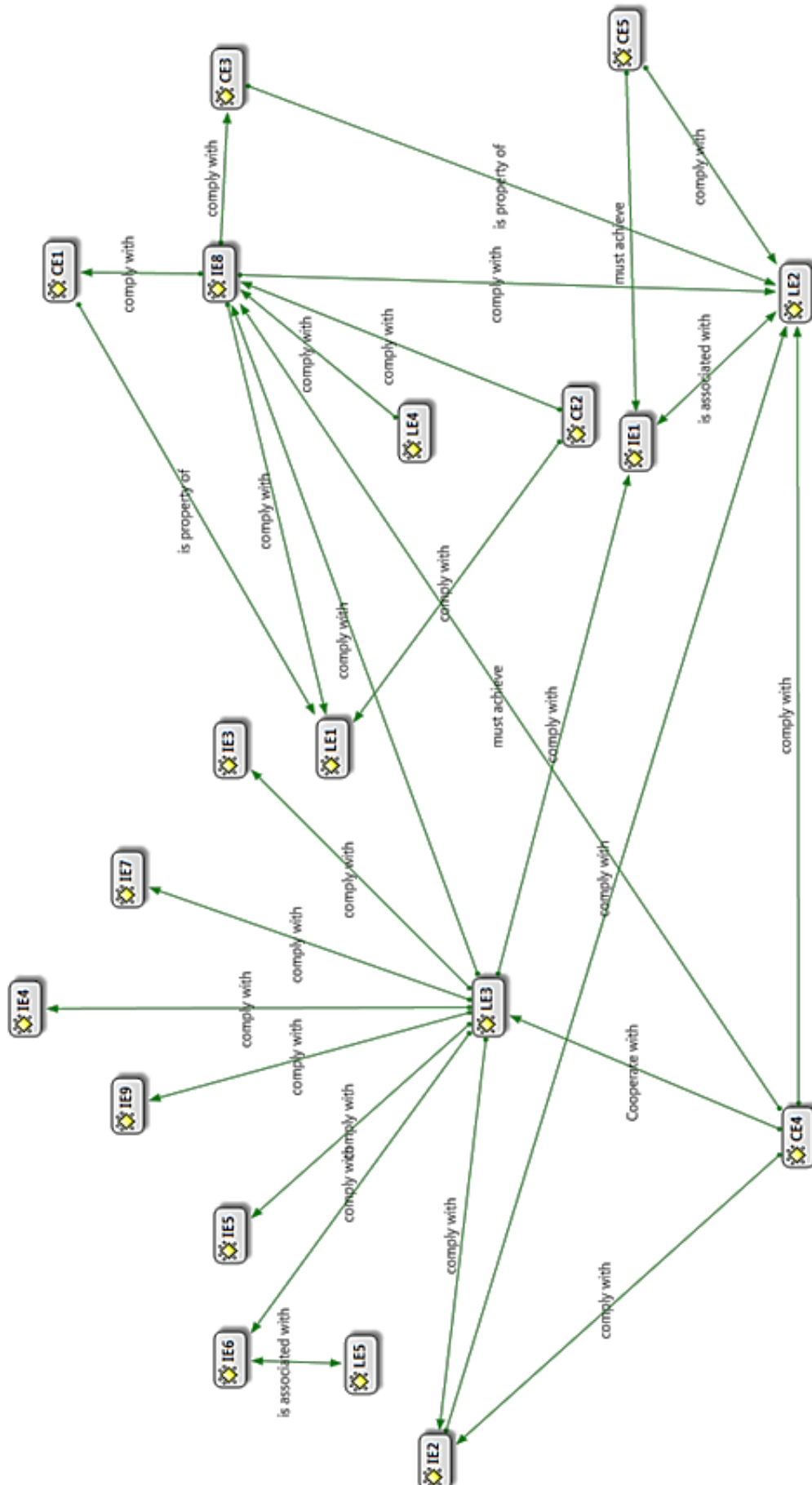


Figure 6: Summary charts of core network groupings from case law wherein electronic evidence was admitted in court.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**6.3.3.1 Interdependencies between Group 1 components**

Findings show three groupings of components under Group 1. These are:

- i. Collection (IE2) and Criminal Process (LE2);
- ii. Justice Personnel (LE5) and Interpretation (IE6) and
- iii. Law Enforcement Agents (LE4) and Presentation (IE8).

The next section presents the interpretation of the interdependencies between each of the Group 1 components.

- i. Collection (IE2) and Criminal Process (LE2): As depicted in Figure 7, the combination of LE2 and IE2 suggests that the nature of the interdependencies between the components speaks to the alignment that needs to exist between evidence collection procedures, as defined by industry (IE2), in order to processes, as stipulated by the law (LE2) of the country. Findings suggest that the function performed by said code family is the collection of evidence. Therefore, the function name was noted as **Evidence Collection**.



Figure 6: Interdependencies between IE2 and LE2

- ii. Justice Personnel (LE5) and Interpretation (IE6): Figure 8 shows the interdependency between components LE5 and IE6. These findings suggest that not only is the burden on industry to correctly interpret (IE6) results stemming from their digital forensic analysis, but that the justice system also has a duty to ensure that digital forensic findings are correctly interpreted, so as to ensure that the law is applied correctly. Findings suggest that the function performed by this code family is the implementation of the justice system. Therefore, the function name was noted as **Justice System Implementation**.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

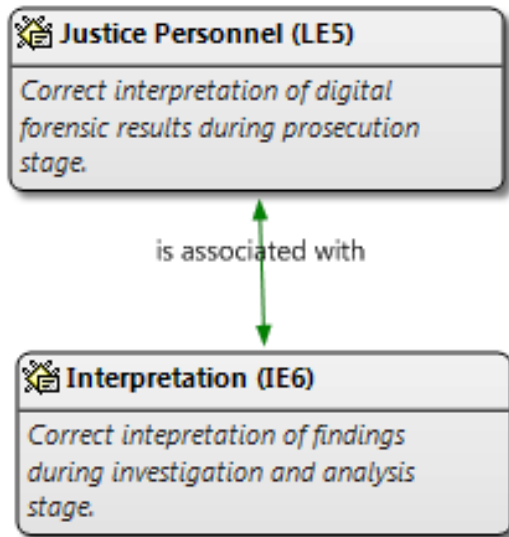


Figure 7: Interdependencies between IE6 and LE5.

- iii. Law Enforcement Agents (LE4) and Presentation (IE8): The last of the Group 1 components is the interdependency between LE4 and IE8. As illustrated in Figure 9, findings suggest that those presenting testimony (IE8) to the courts must be willing, and able, to disclose all which is required by the court. In turn, Law Enforcement Agents (LE4) must be equally willing, and capable, of investigating such crimes. Findings suggest that the function performed by said code family is the prosecution of e-crimes. Therefore, the function name was noted as **e-Crime Prosecution**.

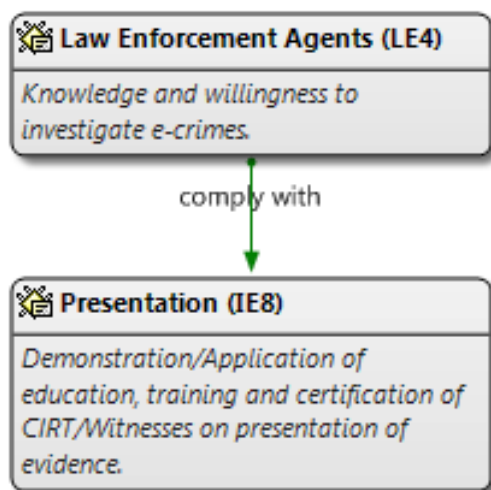


Figure 8: Interdependencies between IE8 and LE4.

The next section discusses the interdependencies between Group 2 components.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**6.3.3.2 Interdependencies between Group 2 components**

Findings show six groupings of components under Group 2. These are:

- i. Human Resources (CE4), Justice System (LE3) and Collection (IE2);
- ii. Presentation (IE8), Standards (CE1) and Electronic Laws (LE1);
- iii. Policies (CE2), Presentation (IE8) and Electronic Laws (LE1);
- iv. Human Resources (CE4), Presentation (IE8) and Criminal Process (LE2);
- v. Presentation (IE8), Procedures (CE3) and Criminal Process (LE2) and
- vi. DFR Technologies (CE5), Preservation (IE1) and Criminal Process (LE2).

The next section presents the interpretation of the interdependencies between each of the Group 2 components.

- i. Human Resources (CE4), Justice System (LE3) and Collection (IE2): As seen in Figure 10, findings suggest that employees (CE4) must be sufficiently trained, educated and certified to operate the organisation’s forensic ready technology, provide witness services and cooperate with those in the justice system (LE3). Additionally, those representing the justice system (LE3) should become fully acquainted with the digital forensic process. Finally, that industry technical experts make use of the correct tools and follow due process in collecting (IE2) evidentiary data. Findings suggest that the function performed by this code family is the handling of evidence. Therefore, the function name was noted as **Evidence Handling**.

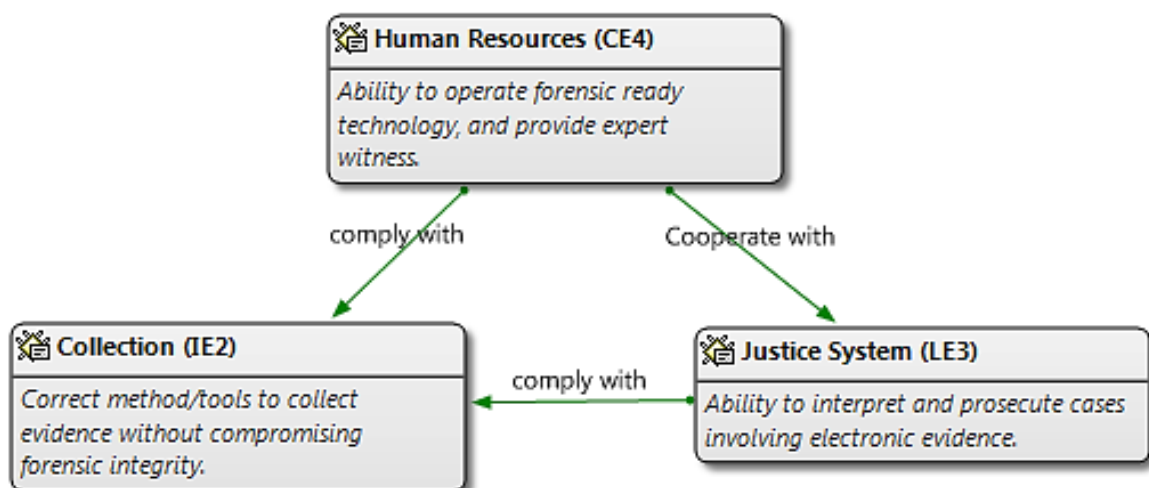


Figure 9: Interdependencies between CE4, LE3 and IE2.

- ii. Presentation (IE8), Standards (CE1) and Electronic Laws (LE1): Findings suggest that

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

the nature of the interdependency within this group of components is such that organisational standards (CE1) need to be developed in line with legislative requirements (LE1). Additionally, the presentation (IE8) of evidence should be in line with organisational standards (CE1). This interdependency is illustrated in Figure 11. Findings suggest that the function performed by the said code family is the localisation of standards. Therefore, the function name was noted as **Standards Localisation**.

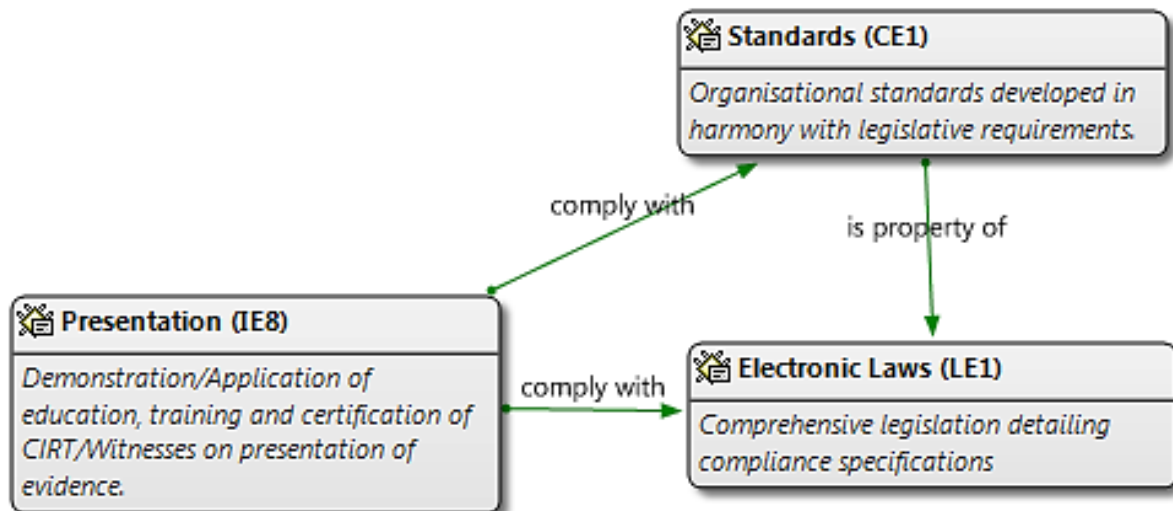


Figure 10: Interdependencies between IE8, CE1 and LE1.

- iii. Policies (CE2), Presentation (IE8) and Electronic Laws (LE1): Findings suggest the need for organisations to develop policies (CE2), in harmony with relevant legislation (LE1), and to ensure that the presentation (IE8) of evidence is in a manner that agrees with relevant legislation (LE1). This interdependency is illustrated in Figure 12. Findings further show that the function performed by this code family is the alignment of policies. Therefore, the function name was noted as **Policy Alignment**.



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

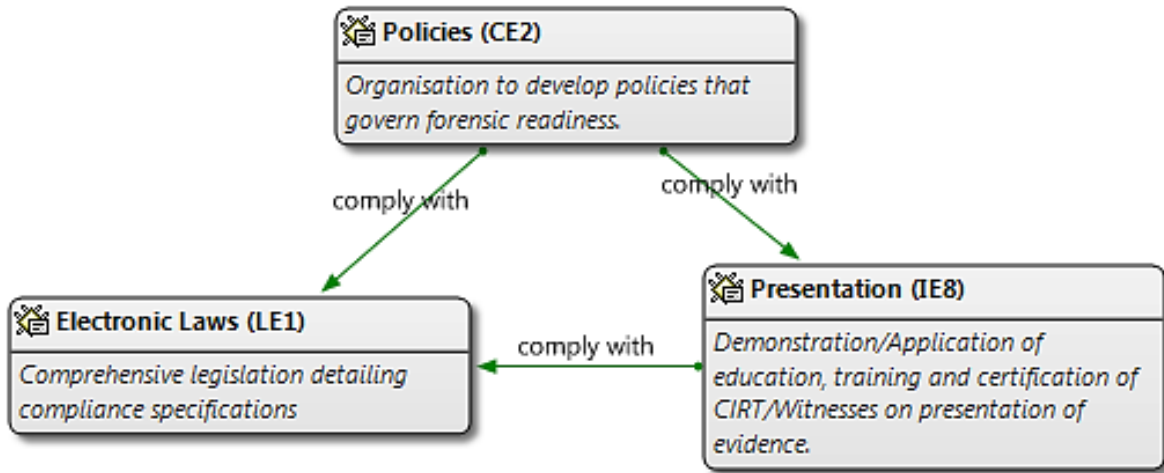


Figure 11: Interdependencies between CE2, IE8 and LE1.

- iv. Human Resources (CE4), Presentation (IE8) and Criminal Process (LE2): As shown in Figure 13, findings suggest that employees (CE4) must be sufficiently trained, educated and certified to operate the organisation’s forensic ready technology, provide witness services (IE8) and cooperate with authorities. Further, that these employees fully comply with the requirements of the criminal process (LE2) and so maintain the evidentiary value of all data processed. Findings suggest that the function performed by this code family is the preparation of witnesses. Therefore, the function name was noted as **Witness Preparation**.

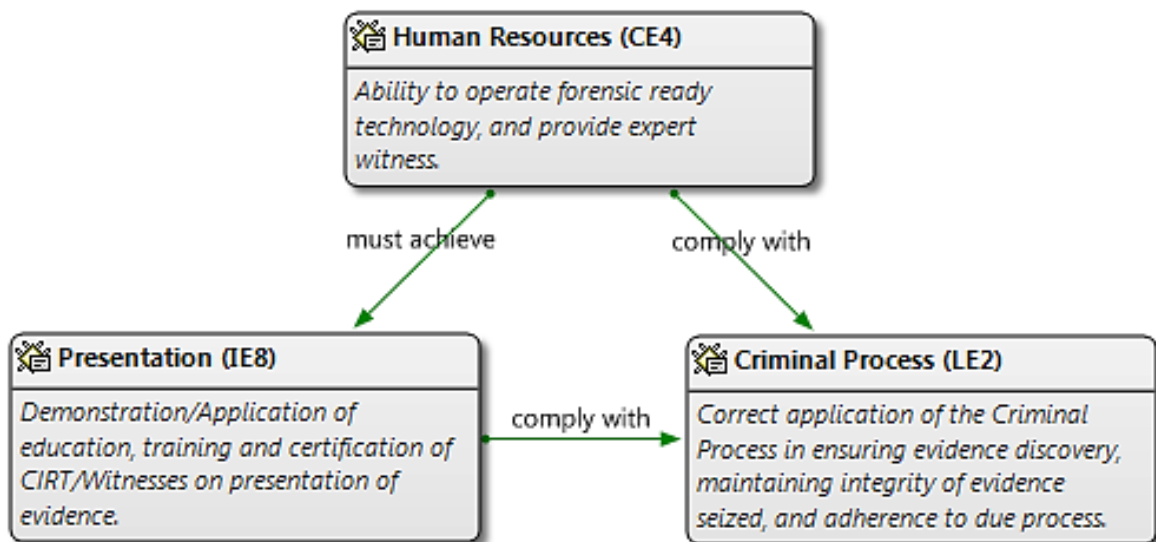


Figure 12: Interdependencies between CE4, IE8 and LE2.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- v. Presentation (IE8), Procedures (CE3) and Criminal Process (LE2): Findings suggest that evidence should be presented (IE8) in such a way that it fully complies with the requirements of the criminal process (LE2) and as stipulated by organisational procedures (CE3). Further, that the latter (CE3) be in harmony with the requirements of the criminal process (LE2) (refer to Figure 14). Findings suggest that the function performed by this code family is the implementation of procedures. Therefore, the function name was noted as **Procedural Implementation**.

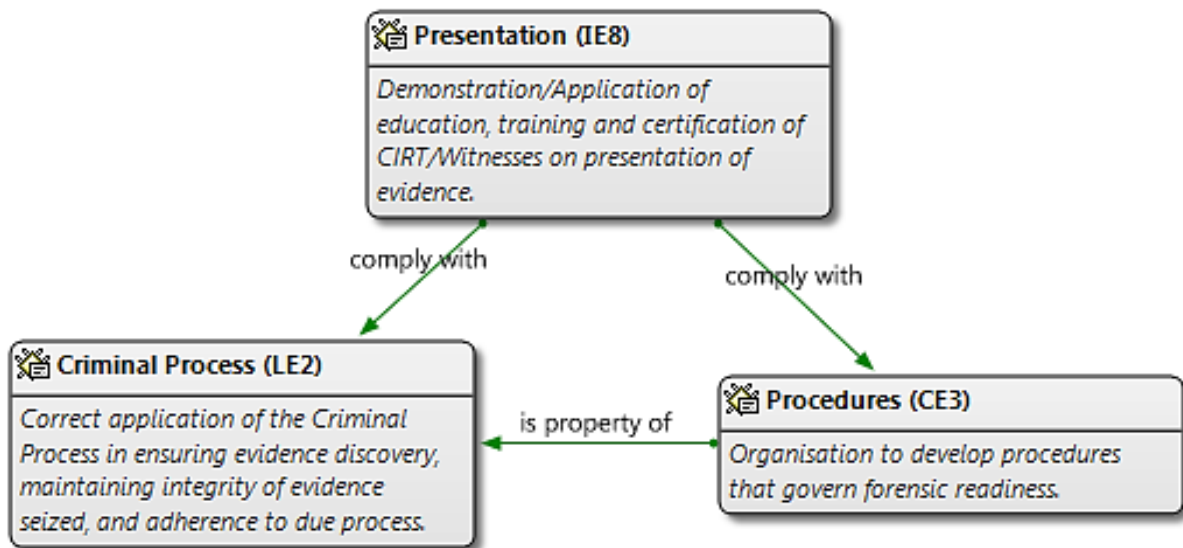


Figure 13: Interdependencies between IE8, CE3 and LE2.

- vi. DFR Technologies (CE5), Preservation (IE1) and Criminal Process (LE2): As shown in Figure 15, findings suggest that the organisation needs to ensure the existence of forensic ready technology (CE5), which preserves (IE1) forensic attributes of all data stored, and maintains evidentiary value as required by the criminal process (LE2). Findings further suggest that the function performed by said code family is the preservation of evidence. Therefore, the function name was noted as **Evidence Preservation**.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

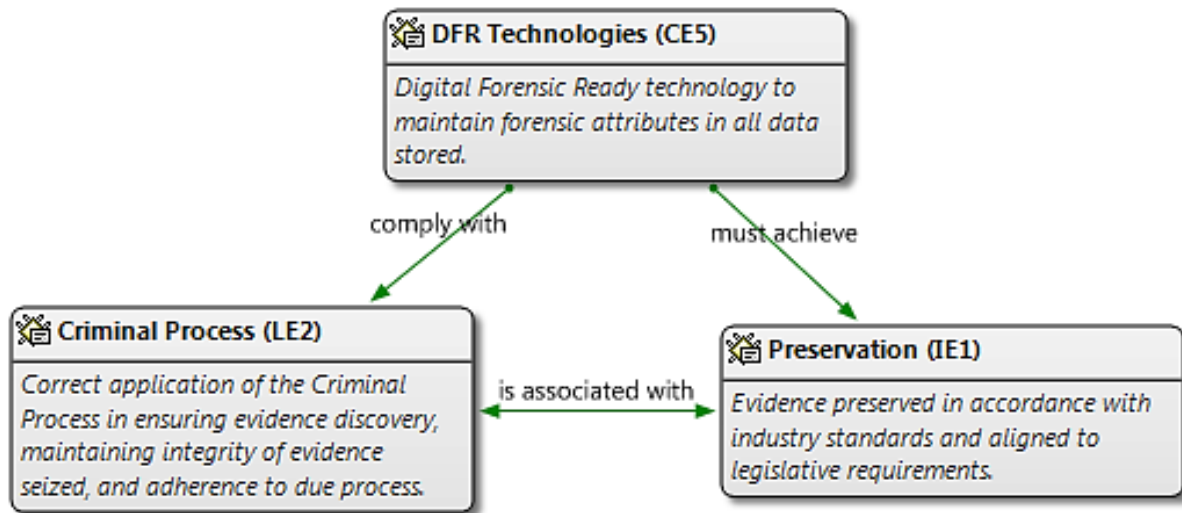


Figure 14: Interdependencies between CE5, IE1 and LE2.

### 6.3.3.3 Interdependencies between Group 3 components

Findings show one grouping of components under Group 3. This entails interdependencies between LE3 and the industry environment, as represented by components IE1, IE2, IE3, IE4, IE5, IE6, IE7, LE8 and IE9.

As illustrated in Figure 16, findings suggest that those in the justice system (LE3) must be adequately acquainted with all aspects of the digital forensic methodology (IE1 to IE9) when prosecuting cases of such a nature. The findings further suggest that the function performed by this code family is the evaluation of the implementation of the digital forensic methodology. Therefore, the function name was noted as **Methodology Evaluation**.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

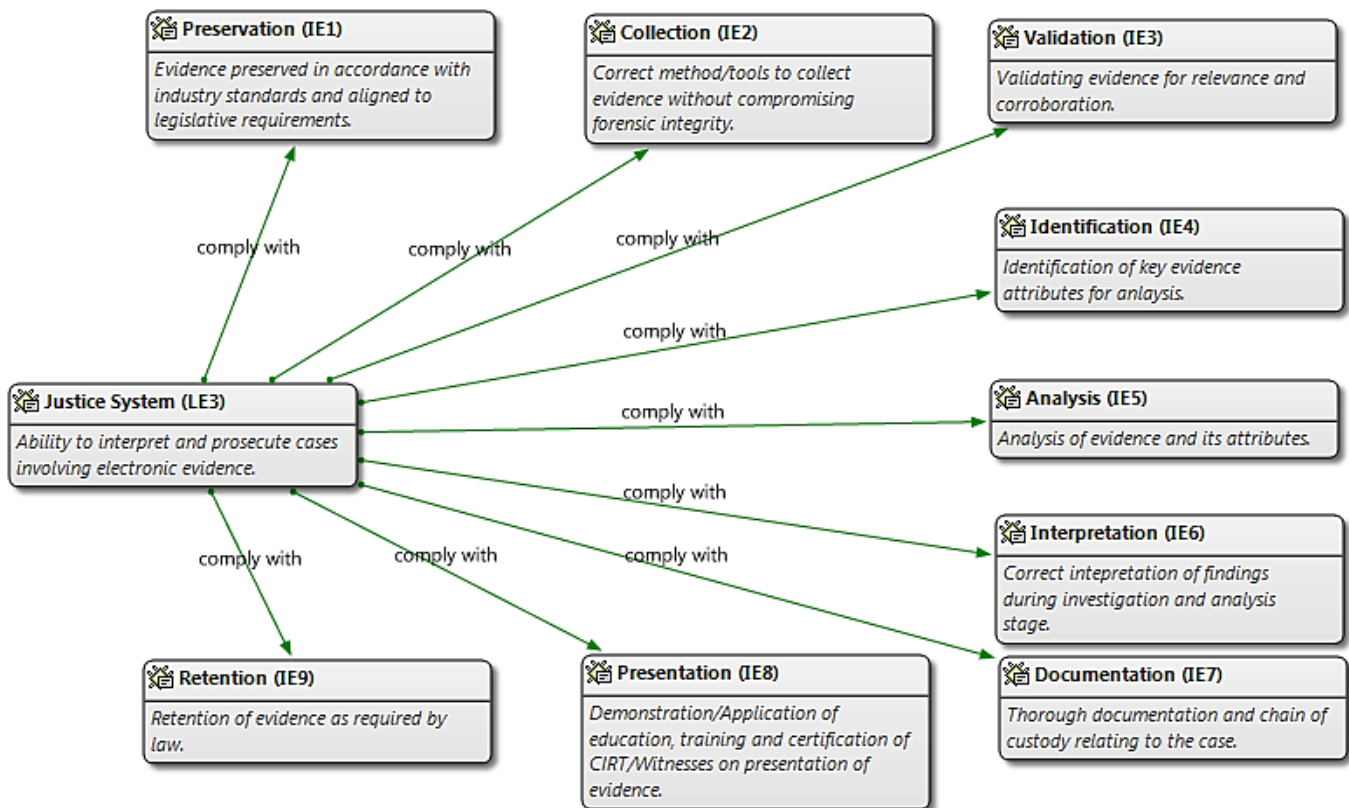


Figure 15: Interdependencies between LE3 and the industry environment as represented by components IE1 to IE9.

The next section presents the final step in applying the conceptual modelling process, i.e. realisation of the conceptual model, and uses an analogy to explain the collective interdependencies which exists between the domains and components discussed.

### 6.4 A Multidisciplinary Conceptual Digital Forensic Readiness Model

In an effort to add clarity to the intricate workings of the proposed model, this section makes use of an analogy wherein the model is compared to the human body. The use of the human body for analogy purposes is deemed appropriate as the proposed model is intended to appeal to a broader audience.

This discussion is followed by the presentation of Figure 17, which is the **Multidisciplinary Digital Forensic Readiness Model (M-DiFoRe)**.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

### 6.4.1 The Analogy

Firstly, consider the impact that *environmental* factors have on the human body. Environmental factors can affect human health in many ways, both positively and negatively.

Then consider the *composition* of the human body, which consists of three key interdependent parts: the head, torso and limbs. According to Camazine et al. (2001) the *physiology* of the head, torso and limbs focuses on individual organs which conduct the body's functions. Walhout et al. (2013) describe the human body as a group of organs or *systems*, that work together to perform a certain task.

Finally, the systems found in the human body self-regulate through a process called homeostasis which maintains stability while adjusting to internal and external conditions (Camazine et al., 2001).

### 6.4.2 Model Functionality

To explain *how* the proposed model works, the study makes use of the above analogy on the workings of the human body.

#### 6.4.2.1 Explanation of Key Concepts

Just as *environmental* factors influence a person's decision to live in one city, rather than another; similarly, when deciding on which environment or **locale** to operate, an organisation needs to carefully consider the impact which factors such as weather, politics, legislation, crime, labour matters and other economic factors will have on its operations. Therefore, the top layer of the M-DiFoRe model is the **Locale**, which requires an organisation to consider factors associated with the environment within which it is established.

The *composition* of the human body can be compared to the three domains of the M-DiFoRe model. Just as adverse changes in weather conditions can negatively affect the human body; once the *general* locale conditions are understood, an organisation will have to investigate *specific* locale conditions (**Domains**) that affect the organisation (Corporate Environment), the industry in which the organisation operates (Industry Environment) and the laws (Legislative Environment) specific to the locale chosen by the organisation. These domains were discussed in chapter 4, section 4.5. This understanding will aid the organisation in preparing for *adverse*

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

*changes*, such as changes in legislation which may impact on the organisation. Therefore, the second layer of the M-DiFoRe model is the **Domain** layer.

Just as the *physiology* of the head, torso and limbs focuses on individual organs which conduct the body's functions; each domain has individual components which are comparable to the organs in the human body. Therefore, the third layer of the M-DiFoRe model is the **Components** layer. These components were discussed in chapter 5, section 5.2.

Finally, as Walhout et al. (2013) explained, the human body is a group of organs or *systems*, that work together to perform a certain task. Therefore, the fourth and final layer of the model is the **Systems** layer. These systems were discussed in chapter 6, section 6.3.3. Just as the human body requires all systems to function properly in order to achieve homeostasis, all systems of the proposed model are important in maintaining forensic readiness.

The consolidation of the four layers discussed above culminate in the Multidisciplinary Digital Forensic Model (M-DiFoRe Model).

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

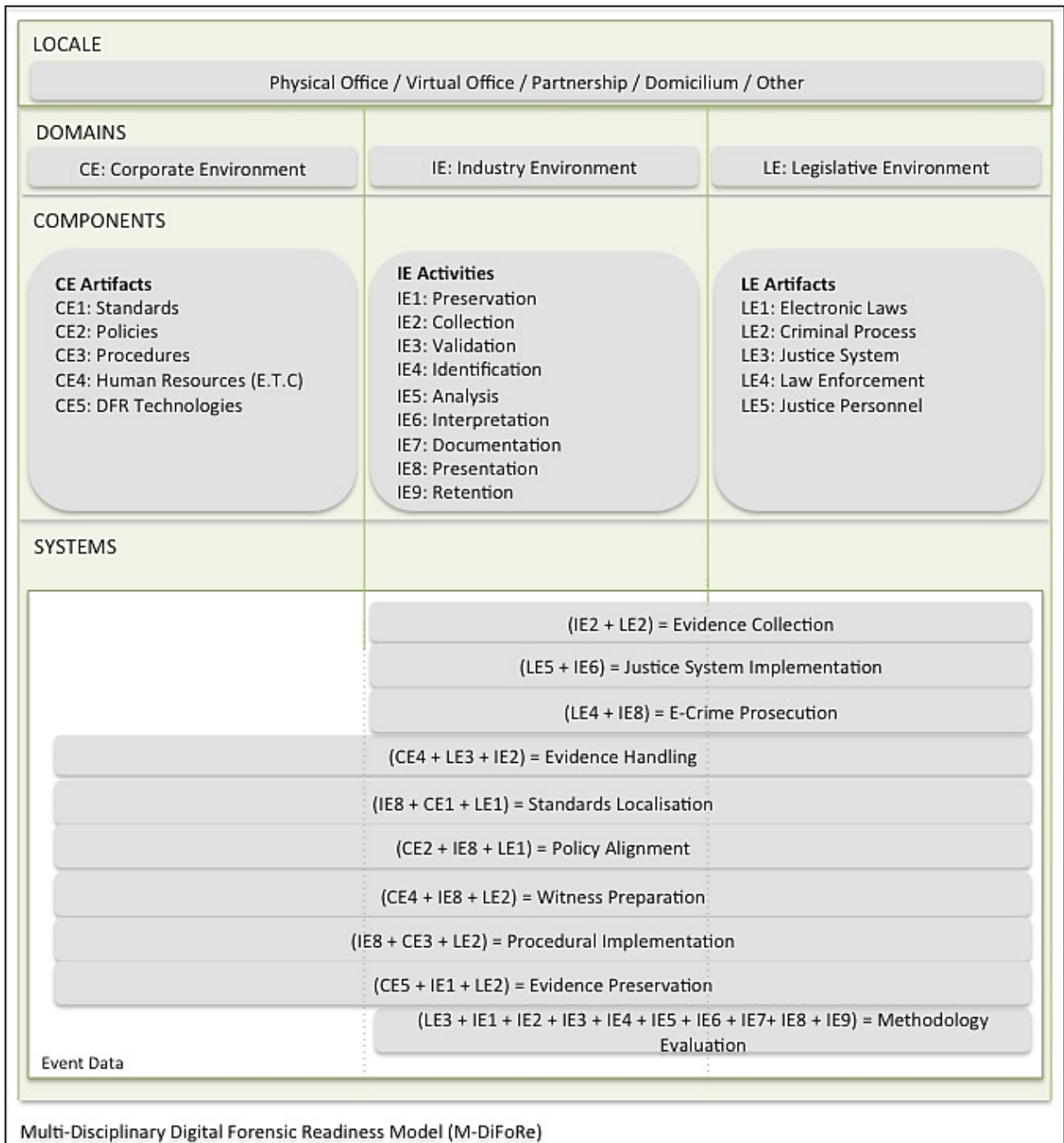


Figure 16: The Multidisciplinary Digital Forensic Model (M-DiFoRe Model).

The section above, together with the previous chapters, provide an explanation as to how the conceptual model was conceived. The next section discusses the application of the conceptual model in order to verify the accuracy and completeness thereof.

#### 6.4.2.2 Applying the Conceptual Model

If a model is to have any practical value, it needs to bridge the gap between the realm of the

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

*conceptual* and the *applied* (Cook, 2005 and Verdonck, 2014). For any organisation to benefit from the M-DiFoRe model, a specific process should be followed in order to achieve the purpose, as set out in section 1.6, Chapter 1.

This section begins with the presentation of a self-assessment tool through which organisations can evaluate their digital forensic readiness, using the M-DiFoRe model as a reference. The self-assessment template (Table 19) lists all the systems (layer 4) of the M-DiFoRe model in addition to four essential steps which analyse the digital forensic readiness of an organisation:

- i. **Step 1:** Establish the existence of each component of the model. This is achieved by:
  - I. *checking* model requirements for each component (column 2) and then conducting a gap analysis to note the existence of each component of the system within the organisation.
  - II. *recording* the results, obtained from the above analysis, in the “Exist” column (column 3) of the self-assessment template (Table 19) with a “Y” indicating that the component exists and a “N” indicating that it does not exist.
  - III. *completing* the “Supporting Evidence Type and Source” column (column 4) by noting the type of evidence to support each finding. The four types of evidence are: Documentary Evidence (D), Observed Processes (P), Verbal Statements (S) and Appendices (A). The source of the evidence is also to be noted. The types of supporting evidence and related abbreviations are explained at the end of this section.
- ii. **Step 2:** Establish the existence of each system (column 1) which is achieved by:
  - I. *completing* the “Exist” column (column 5) found under step 2 (Table 19) and entering a “Y” where *all* the components of the system exist, as per the findings from step 1. However, if step 1 reveals that one, or more, components were missing, then the system has to be marked as incomplete by entering a “N” in the “Exist” column.
  - II. *completing* the “Supporting Evidence Type and Source” column (column 6) by noting the type of evidence to support each finding, as well as its source.
- iii. **Step 3:** Establish the nature of the interdependencies which were found to exist between the existing systems. In the case of systems that do not exist, skip to step 4. This step is achieved by:
  - I. *completing* the “Link type” column (column 7.2). This is achieved by noting the component pair and entering the link type abbreviation in accordance with the guidelines provided in Table 18.
  - II. *completing* the “Arrow type” column (column 7.3). This is achieved by entering



## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

the type of arrow which represents the information flow between the component pair under analysis, as per the guidelines provided in Table 18.

III. *completing* the “Model Compliance” column (column 8) by determining the degree to which the system under analysis complies with the requirements of the model.

Results are noted under only one of three possible classifications, namely:

- a. None: where the system interdependencies within the organisation do not agree with those of the model.
- b. Partial: where there is a partial alignment between what has been found within the organisation and that which the model stipulates.
- c. Full: where the system found *that* within the organisation to be exactly as defined by the M-DiFoRe model.

IV. *completing* the “Supporting Evidence Type and Source” column by noting the type of evidence which supports each finding, as well as its source.

- iv. **Step 4:** Where findings from Model Compliance (column 8) reflect a “None” or “Partial” compliance, corrective steps are to be taken in accordance with the guidelines provided by the M-DiFoRe model (Chapter 6, section 6.3.3). Step 4 concludes the self-assessment process and requires that remedial action be undertaken to correct vulnerable systems. Reference to the theory, which contains the requirements of the model, is noted under the “Model reference” column (column 11).

Based on the previous assessment, a detailed action plan can be developed to guide those activities required towards increasing an organisation’s digital forensic readiness.

With the execution of steps 1 to 3, as detailed above, it is imperative to collate sufficient and appropriate evidence to support and substantiate findings. It is of the utmost importance to note that there can be more than one possible evidence type to support a finding. Therefore, a description as to the nature of the source must be added for each type of evidence selected from the four options which follow. Appropriate supporting evidence types are:

- i. Documentary evidence (D) such as documents created by the organisation in the normal course of business, policies and transactional data. This is abbreviated as “D” in the “Supporting Evidence Type and Source” columns (columns 4, 6 and 10) of the self-assessment template. Documentary evidence is classified as real evidence and carries material evidentiary weight in court.
- ii. Observed processes (P) and physical items, such as monitoring the operation of an intrusion detection system, or physically inspecting a collection of storage media containing archived firewall logs. This is abbreviated as “P” in the “Supporting

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

evidence” column of the self-assessment template. The observation is carried out by the person applying the self-assessment. Observing a process may be necessary to confirm a finding which emanates from documentary evidence.

- iii. Verbal statements (S) include comments or references made by organisational representatives as to the existence of processes and procedures. This is abbreviated as “S” in the “Supporting Evidence Type and Source” column of the self-assessment template. To maintain evidentiary weight, it is necessary for the person applying the self-assessment to obtain verbal statements directly from the source.
- iv. Appendices (A) are documents external to the organisation and are created by the person applying the self-assessment during the M-DiFoRe model implementation process. Appendices should detail the thought process applied during analysis, evidence of research conducted and data analysis reports generated in the course of applying the self-assessment. This is abbreviated as “A” in the “Supporting Evidence Type and Source” column of the self-assessment template.

Table 19 illustrates the self-assessment template, with the model’s systems and components as pre-populated fields against which the assessment is based.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

(1) M-DiFoRe Systems	Component Existence (Step 1)				System Existence (Step 2)				System Interdependencies (Step 3)						Remediation (Step 4)					
	(2) Component Name	(3) Exist (Y/N)	(4) Supporting Evidence Type & Source				(5) Exist (Y/N)	(6) Supporting Evidence Type & Source				(7) Nature of dependency			(8) Model Compliance (N,P,F)	(9) Supporting Evidence Type & Source				(10) Model Reference
			D	P	S	A		D	P	S	A	(7.1) Links	(7.2) Link Type (Co, Coo, Pr, Ac, As)	(7.3) Arrow Type (Uni-D, Bi-D)		D	P	S	A	
Evidence Collection (IE2, LE2)	IE2: Collection											L2, IE2								
	LE2: Criminal Process																			
Justice System Implementation (LE5, IE6)	LE5: Justice Personnel											LE5, IE6								
	IE6: Interpretation																			
e-Crime Prosecution (LE4, IE8)	LE4: Law Enforcement											LE4, IE8								
	IE8: Presentation																			
Evidence Handling (CE4, LE3, IE2)	CE4: Human Resources											CE4, LE3								
	LE3: Justice System											CE4, IE2								
	IE2: Collection											LE3, IE2								
Standards Localisation (IE8, CE1, LE1)	IE8: Presentation											IE8, CE1								
	CE1: Standards											CE1, LE1								
	LE1: Electronic Laws											IE8, LE1								
Policy Alignment (CE2, IE8, LE1)	CE2: Policies											CE2, IE8								
	IE8: Presentation											IE8, LE1								
	LE1: Electronic Laws											CE2, LE1								
Witness Preparation (CE4, IE8, LE2)	CE4: Human Resources											CE4, LE2								
	IE8: Presentation											CE4, IE8								
	LE2: Criminal Process											IE8, LE2								
Procedural Implementation (IE8, CE3, LE2)	IE8: Presentation											IE8, CE3								
	CE3: Procedures											IE8, LE2								
	LE2: Criminal Process											CE3, LE2								
Evidence Preservation (IE8, CE3, LE2)	CE5: DFR Technologies											CE5, IE1								
	IE1: Preservation											LE2, IE1								
	LE2: Criminal Process											CE5, LE2								
Methodology Evaluation (LE3, IE1-IE9)	LE3: Justice System											-								
	IE1: Preservation											LE3, IE1								
	IE2: Collection											LE3, IE2								
	IE3: Validation											LE3, IE3								
	IE4: Identification											LE3, IE4								
	IE5: Analysis											LE3, IE5								
	IE6: Interpretation											LE3, IE6								
	IE7: Documentation											LE3, IE7								
	IE8: Presentation											LE3, IE8								
IE9: Retention											LE3, IE9									

Table 19: Self-Assessment template for using the M-DiFoRe model to identify vulnerable systems.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

In view of the results of the self-assessment process, the model provides a guideline according to which an organisation can ensure that the necessary components and systems are in place. Additionally, the model helps with an understanding of the respective functions of these components and systems. This process is non-linear, thus allowing the organisation to implement the model starting at any layer as based on priorities identified in the self-assessment.

The next section discusses the key differentiators from previous models presented.

### **6.5 M-DiFoRe Model Key Differentiators**

In Chapter 2, section 2.2.5, an overview is provided of various digital forensic models that were developed since 2001. The M-DiFoRe model differentiates itself from these models in the following ways:

#### **6.5.1 Systematic Classification of Critical Components**

The models reviewed as part of this study present varying components derived from a bottom-up technical approach. As per Table 5, models 1-4,6,7,11 and 13 were developed using a bottom-up approach. The M-DiFoRe model was developed with the end in mind (top-down), and made use of a case-law-driven approach to extrapolate critical components, as observed from the way in which the courts processed digital evidence. This facilitated the identification of common factors which the courts considered important in determining the admissibility and weight of evidence led. Several examples of case law were analysed in chapter 6 and with the aid of Atlas.ti, the coded data was systematically classified to arrive at an inclusive list of critical components and the systems or families to which they belong.

The practical value derived from this approach is that the risk of negating evidentiary data is reduced, through the holistic identification and prioritisation of critical components. This requirement is in line with the Purpose Statement as detailed in Chapter 1.

#### **6.5.2 Strategic Codification of Component Interdependencies**

Pursuant to the identification and classification of critical components was the strategic codification of the same, in order to investigate component interdependencies. The M-DiFoRe model identifies components with one-to-one, one-to-many and other types of dependencies, as discussed in Chapter 5. This sets the M-DiFoRe model apart from existing reviewed models

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

5-13 as shown in Table 5, as it provides deeper insight into the ripple effect which a change in the state of an attribute of a component has in relation to other associated components of the model.

In line with the Problem Statement, this addresses the gap noted, by providing an enhanced multidisciplinary approach which seeks to identify inter-disciplinary interdependencies, thereby reducing the organisational risk of inadvertently destroying evidence.

### **6.5.3 Cross-Functional Approach with Multiple Starting Points**

Unlike the process-based and integrated models 5, 7-13 discussed in Table 5, the M-DiFoRe model does not have a single starting point for implementation. Each system of the model is in itself a starting point and represents a complete module that can function independently without the need to implement the model in its entirety.

This facilitates a phased implementation approach, based on the needs of the organisation, rather than simply applying a process from beginning to end before deriving value. Furthermore, the existence of multiple starting points in the M-DiFoRe model facilitates parallel implementation of systems for increased optimisation of organisational digital forensic readiness.

Finally, in line with the Problem Statement, this modularity in design reduces the complexities associated with achieving digital forensic readiness by subdividing the implementation into smaller independent parts.

### **6.5.4 Non-Context Specific (Universal) Application**

The M-DiFoRe model deviates from the trend noted in models 8, 10 and 13 as discussed in Table 5, which tend to be context and use case specific.

The practical value derived is that M-DiFoRe model assumes a macro integrated approach which focuses on digital forensics as a discipline, thereby applying a principle-based design to enhance its applicability across different disciplines.

In line with the Problem Statement, this provides a more universal way of addressing the multidisciplinary nature of digital crimes as it can be applied to any type of organisation using

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

any type of technology.

### **6.6 Conclusion**

The primary goal of this chapter is the realisation of the conceptual model as the final step in applying the conceptual modelling process. The secondary goal is to verify the accuracy and completeness of the blueprint (Table 15, Chapter 4, page 75) which identifies the domains and their respective components, as presented in Chapter 5. This verification process was done through a review of three legal cases which were heard in the South African courts (section 6.3).

The interpretive paradigm as discussed in chapter 2 was used to analyse secondary research data (Case Law) that was utilised for purposes of verifying prior primary research findings. The results of this process confirmed that the identified 18 components, 10 systems, and their respective domains, were present in all cases analysed and that no new components or domains emerged.

Additionally, this chapter identified the interdependencies between the components, the systems and their respective domains in order to develop the multidisciplinary conceptual model. Findings show ten systems, which are made up of more than two components from different domains, which self-regulate to maintain digital forensic homeostasis within an organisation.

The chapter also verifies the accuracy and completeness of the blueprint presented in Table 15 by triangulating findings from chapter 2, using a different research method and arriving at the same results.

This chapter concludes with the presentation of the M-DiFoRe model. It uses the analogy of the human body to explain *how* the proposed model can be applied in order to enable organisations to reduce likely dangers from the unintended destruction and negating of evidentiary data as per the purpose statement in Chapter 1, section 1.6. In addition, the study provides a process on how an organisation can use the proposed model to conduct a self-assessment.

The next chapter is concerned with the validation of the proposed model, and tests the proposed

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

model against a different case that met the same selection criteria as those presented in this chapter, but where the court found the electronic evidence presented inadmissible. The purpose of this to determine whether the proposed model could have prevented this from happening as per the purpose statement in Chapter 1, section 1.6.



## **7. Chapter 7: Model Validation Approach**

---

### **7.1 Introduction**

The previous chapter presented and explained the realisation of the conceptual model and verified the accuracy and completeness of the proposed model, as derived from an analysis of case law in Chapter 6 wherein the courts found electronic evidence admissible. The aim of this chapter is to *validate the proposed model*, using a different case where the courts found electronic evidence presented *inadmissible*. The said validation process uses the implementation tool as discussed in section 6.4.2.2. The application of the proposed model to a case such as this demonstrates the difference the model can make in the admissibility of evidence.

This chapter presents evidence which suggests that the proposed model is *sufficiently accurate for its intended use* of enabling organisations to reduce the potential dangers from the inadvertent destruction and negating of evidentiary data, and improving overall organisational digital forensic readiness.

The evidence stems from an analysis of case law, as presented in the South African courts, wherein electronic evidence formed a key part of evidence led during legal proceedings. Unlike the three cases in Chapter 6, the case used for validating the model contained digital evidence that the court deemed inadmissible. If applying the model to this case results in the identification of the components and inherent relationships that caused the evidence to be inadmissible, the model can be considered valid and sufficiently accurate.

The chapter starts by presenting a *synopsis* of the legal case used. This discussion is followed by a *post-analysis* of the case using the proposed model, to thereby determine the validity of the model in preventing the organisation from inadvertently destroying or negating evidence. The chapter concludes with a *discussion of the results of the validation process* and identifies critical points of failure in the case which, if the model had been applied before the events, could have mitigated the risk of the organisation inadvertently negating evidentiary data, thus losing the case.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

### **7.2 Validation Protocol**

As Debbabi et al. (2010) and Verdonck (2014) explained, model validation is undertaken to build confidence and credibility, and is the final step in the applied modelling process, as discussed in section 5.3.2, step 6.

This is achieved in this section, by applying the model (retrospectively), to a case that was presented in court, wherein electronic evidence was found inadmissible. The validation is done based on a two-pronged approach to achieve the same goal. The first method uses the self-assessment template presented in chapter 6. The second method is based on a qualitative analysis of the case using ATLAS.ti. If a comparing of the results obtained from the two methods show a high degree of similarity, the model can be considered as sufficiently valid. Discrepancies in the results would invalidate the model.

Key activities undertaken in the validation process are:

- i. Activity 1 - Present case law synopsis where electronic evidence was found inadmissible;
- ii. Activity 2 - Apply steps 1 to 3 of the self-assessment template to the said case law;
- iii. Activity 3 - Perform a qualitative analysis on the said case law;
- iv. Activity 4 - Compare results from activity ii and iii above and
- v. Activity 5 - Apply step 4 of the self-assessment template to the said case law.

### **7.3 Validation of model**

This section presents the analysis of the court case in question. (Refer to Appendix 8 for the full court case).

#### **7.3.1 Activity 1 - Case Law Synopsis: Defamation and Unlawful Competition**

In this case, the applicants alleged that the respondent had sent an email to its customers, competitors and staff which was defamatory and which interfered with its contractual relationships (Juta Law, 2016). The case is in the public domain and therefore complies with the ethics requirements as discussed in Chapter 1, section 1.7.

The respondent was employed by the applicant from 2010 as a software developer and later became its Chief Information Officer. The respondent resigned with effect 31 January 2014. On termination of his employment, the respondent was subject to a restraint of trade agreement,

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

precluding him from doing business with certain of the applicant's customers. The applicant alleged that subsequent to the termination of his employment, the respondent had motive to harm the applicant's business as he resigned before being eligible to receive a bonus of R11 million (\$900k).

Based on the above, the applicants obtained a court order allowing for a search of the respondent's premises, the seizure of relevant documents (and their preservation) pending an action which it intended to initiate against the respondent for defamation and unlawful competition.

An issue on the return day of the hearing was the degree of proof that the applicants were required to show in respect of the requirements for the order, namely:

- i. Possession by the respondent of vital evidence;
- ii. A real apprehension that it might have been hidden or destroyed and
- iii. A cause of action to which the evidence related.

The court ruled that the applicants had failed to establish a strong prima facie case that the respondent was the author of the defamatory emails in question, or that he had, what the applicant deemed intellectual property. The preservation order was accordingly discharged (Juta Law, 2016).

### **7.3.2 Activity 2 - Self Assessment**

This section presents an application of the steps as detailed in section 6.4.2.2.

#### **7.3.2.1 Step 1: Component Existence**

The application of the M-DiFoRe model begins with conducting a gap analysis into the existence of the relevant components within the organisation. In this instance, the process entailed a review of case law, as per section 7.3.1, with the objective of extrapolating supporting evidence (section 6.4.2.2) which indicates the presence of each of the components of the M-DiFoRe Model.

Table 20 shows partial results (5 systems only) of the completed self-assessment (step 1). The results suggest that all components of the model were found to exist in the case analysed. The

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

complete self-assessment results can be viewed in Appendix 9.

		<b>Component Existence (Step 1)</b>				
(1) M-DiFoRe Systems	(2) Component Name	(3) Exist (Y/N)	(4) Supporting Evidence Type & Source			
			D	P	S	A
Evidence Collection (IE2, LE2)	IE2: Collection	Y	1, 4			1, 23 -25
	LE2: Criminal Process	Y	1, 6, 21			
Justice System Implementation (LE5, IE6)	LE5: Justice Personnel	Y	2			
	IE6: Interpretation	Y	1		11, 12	1
e-Crime Prosecution (LE4, IE8)	LE4: Law Enforcement	Y	2			
	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1
Evidence Handling (CE4, LE3, IE2)	CE4: Human Resources	Y	8, 9			
	LE3: Justice System	Y	1, 2, 5, 7, 26		32	
	IE2: Collection	Y	1, 4			1, 23 - 25
Standards Localisation (IE8, CE1, LE1)	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1
	CE1: Standards	Y	1			
	LE1: Electronic Laws	Y	1, 3, 22			

Table 20: Step 1: Self-Assessment Results

Results in column 3 (Exist) indicates a “Y” which denote that all the components were found to exist, as per the model guidelines. Furthermore, the Supporting Evidence Type and Source (column 4) is listed as documentary evidence (D) presented to the court, verbal statements (S) and appendices (A), which include evidence found by law enforcement during the course of the investigation. The number/s in column 4 indicate the section in the case law where evidence of the existence of a component was found (see Appendix 9, column 4).

The application of identifying “System Existence” (step 2) is discussed next.

### 7.3.2.2 Step 2: System Existence

The next activity is to establish the existence of each system, as shown in Table 21.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

The execution of step 2 requires that the “Exist” column (column 5) be completed to indicate the presence or absence of a system, followed by “Supporting Evidence Type and Source” (column 6). In this case, Table 21 (step 2, column 5) shows that all the systems of the model were found to exist, and that supporting evidence (column 6) is documentary evidence (D), verbal statements (S) and appendices (A), as previously discussed in step 1.

Since the self-assessment process was applied retrospectively to case law, it was necessary to analyse the case using an approach detailed enough so that the nuances of the case could stand out. For this reason, techniques from immersion/crystallisation and constant comparison, as discussed in Chapter 4 and applied to the interview transcripts, were applied to aid in the identification of the systems of the model, and the type of evidence that was presented to the courts. The iterative reading process made it possible for focus/immersion to be applied to each paragraph of case law and for the emergence/crystallisation of findings to take place.

Since the fully completed self-assessment document is lengthy, only the results of the first 5 systems are shown in Table 21. Appendix 9 contains the complete self-assessment.

Step 2 is an important step as it lays the foundation for comparison with the qualitative analysis, which ultimately determines the validity of the manual analysis process (Table 19). Similarity in results between the latter and Figure 17, would not only validate the M-DiFoRe model, but also the process of applying the model, as discussed in section 6.4.2.2.

Table 21 is presented next, followed by the application of step 3 of the self-assessment.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

(1) M-DiFoRe Systems	Component Existence (Step 1)						System Existence (Step 2)				
	(2) Component Name	(3) Exist (Y/N)	(4) Supporting Evidence Type & Source				(5) Exist (Y/N)	(6) Supporting Evidence Type & Source			
			D	P	S	A		D	P	S	A
Evidence Collection (IE2, LE2)	IE2: Collection	Y	1, 4			1, 23 -25	Y	1, 4, 6, 21			1, 23-25
	LE2: Criminal Process	Y	1, 6, 21								
Justice System Implementation (LE5, IE6)	LE5: Justice Personnel	Y	2				Y	1, 2		11 ,12	1
	IE6: Interpretation	Y	1		11, 12	1					
e-Crime Prosecution (LE4, IE8)	LE4: Law Enforcement	Y	2				Y	1, 2, 30		11, 12, 15-20, 33-36	1
	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1					
Evidence Handling (CE4, LE3, IE2)	CE4: Human Resources	Y	8, 9				Y	1, 2, 4, 5 7-9, 26		32	1, 23-25
	LE3: Justice System	Y	1, 2, 5, 7, 26		32						
	IE2: Collection	Y	1, 4			1, 23 - 25					
Standards Localisation (IE8, CE1, LE1)	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1	Y	1, 3, 22, 30		11, 12, 15-20, 33-36	1
	CE1: Standards	Y	1								
	LE1: Electronic Laws	Y	1, 3, 22								

Table 21: Step 2: Self-Assessment Results

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

### 7.3.2.3 Step 3: System Interdependencies

The aim of this step is to establish the nature of the interdependencies which exist between the systems which were found to exist. Following guidelines, as per section 6.4.2.2, Table 22 shows the “Link type” (column 7.2) and associated “Arrow type” (column 7.3) for each of the systems analysed.

Findings relating to the degree in which the systems under analysis comply with the requirements of the model are shown in column 8 (Model Compliance) and note that supporting evidence (column 9) is documentary evidence (D), verbal statements (S) and appendices (A). The theory which elucidates the differences in these evidence types is presented in section 6.4.2.2. The number/s in column 9, indicate the paragraph in the case law where evidence of the existence of a system was found. Appendix 9, column 9 contains the complete list of supporting evidence.

The process identified system interdependency issues relating to the evidence preservation system. This suggests that the nature of the interdependency between components CE5 and IE1 is not in accordance to what the M-DiFoRe model proposes. This is the only system which was found to be **noncompliant** with the M-DiFoRe model.

Further findings show six systems with instances of **partial compliance** and nine instances of **full compliance** with the M-DiFoRe model. The model proposes that noncompliant and partially compliant systems be remediated during step 4, with the objective making them fully compliant.

As with the previous steps, only the results of the first 5 systems are shown in Table 22. See Appendix 9 for the complete self-assessment.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

System Interdependencies (Step 3)								
(1) M-DiFoRe Systems	(7) Nature of dependency			(8) Model Compliance (N,P,F)	(9) Supporting Evidence Type & Source			
	(7.1) Links	(7.2) Link Type (Co, Coo, Pr, Ac, As)	(7.3) Arrow Type (Uni-D, Bi-D)		D	P	S	A
Evidence Collection (IE2, LE2)	L2, IE2	Co	Uni-D	F	1, 4, 6, 21			1, 23-25
Justice System Implementation (LE5, IE6)	LE5, IE6	As	Bi-D	F	1, 2		11, 12	1
e-Crime Prosecution (LE4, IE8)	LE4, IE8	Co	Uni-D	F	1, 2, 30		11, 12, 15-20, 33-36	1
Evidence Handling (CE4, LE3, IE2)	CE4, LE3	Coo	Uni-D	F	1, 2, 5 7, 8, 9 26		32	
	CE4, IE2	Co	Uni-D	P	1, 4, 8, 9			1, 23-25
	LE3, IE2	Co	Uni-D	F	1, 2, 4, 5, 7, 26		32	1, 23-25
Standards Localisation (IE8, CE1, LE1)	IE8, CE1	Co	Uni-D	F	1, 30		11, 12, 15-20, 33-36	1
	CE1, LE1	Pr	Uni-D	F	1, 3, 22			
	IE8, LE1	Co	Uni-D	P	1, 3, 22, 30		11, 12, 15-20, 33-36	

Table 22: Step 3: Self-Assessment Results



### **7.3.3 Activity 3 - Qualitative Analysis**

In addition to manually applying the self-assessment for purposes of demonstrating the M-DiFoRe model's basic application within an organisation, it was necessary to qualitatively analyse the case law, as summarised in section 7.3.1. This qualitative data analysis used the Atlas.ti tool which enables a comparison of the results of the two different methods applied. The qualitative analysis uses the data analysis method, as discussed in Chapter 4, section 4.3.2.

Figure 18 illustrates that the validation process identified system vulnerabilities. Green solid information flow lines indicate full compliance to the requirements of the model. On the other hand, red solid information flow lines indicate partial compliance to the requirements of the model and red dotted lines indicate a gap, or complete noncompliance.

Since the purpose of this chapter is to validate the proposed model, the same codes tabulated in Table 15 (Chapter 4, section 4.5.4.4) were used. Findings from Figure 18 show that:

- i. Twelve component pairs were found to be **fully compliant** with the requirements of the model and only. From these, only 3 systems were found to be fully compliant.
- ii. A further 12 component pairs have a red solid information flow line which, as discussed, indicates **partial compliance** to the requirements of the model. From this, only 6 systems were found to be partially compliant.
- iii. Only 1 system was found to have a **noncompliant** component pair, as indicated by a red dotted line.

The following sub sections present the findings of the detailed analysis in order to arrive at the results illustrated in Figure 18.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

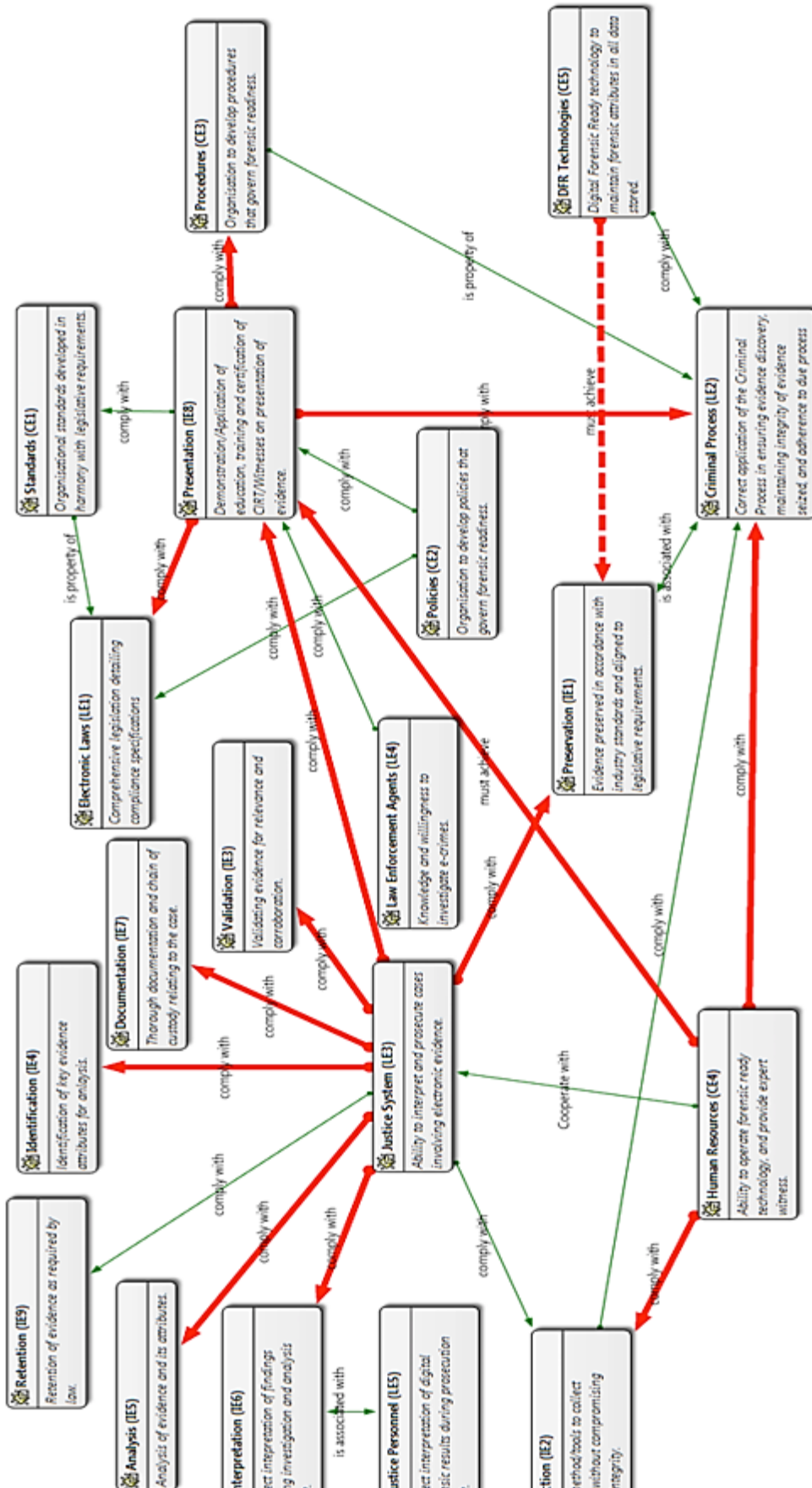


Figure 18: Summary chart of core network groupings on case law that where electronic evidence was found inadmissible by the court

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

### 7.3.3.1 Evidence Collection System (IE2 to LE2)

An evaluation of this system shows that correct methods and tools were used to maintain evidence integrity, and that this was executed *in accordance with* the requirements of the Criminal Process (see Figure 19).

Findings show that the investigators met the requirements set out by components (IE2) and (LE2), as required by the model, resulting in the court accepting that the integrity of the evidence presented had been maintained.

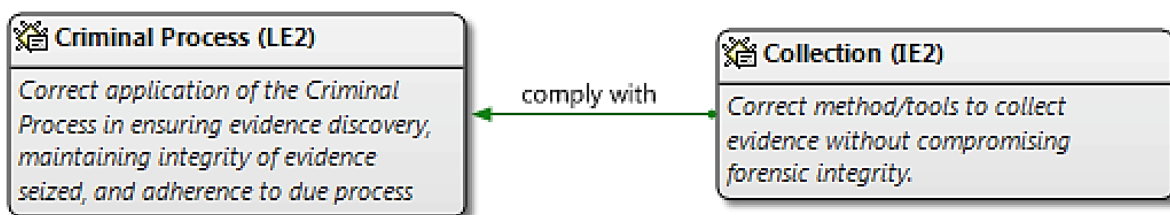


Figure 17: Analysis of the Evidence Collection system.

Therefore, the result of the self-assessment is that all components of the model exist, as defined by the M-DiFoRe model, and thus a *full compliance* rating was noted against this system.

### 7.3.3.2 Justice System Implementation System (LE5 and LE6)

Findings which stem from the evaluation of this system show that Justice Personnel could correctly interpret findings presented and, in addition, interrogate the way the digital forensic methodology was applied. Similarly, those representing the industry environment were able to present their interpretation of findings in a way that allowed the Justice Personnel to understand and interrogate the process followed (see Figure 20).

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

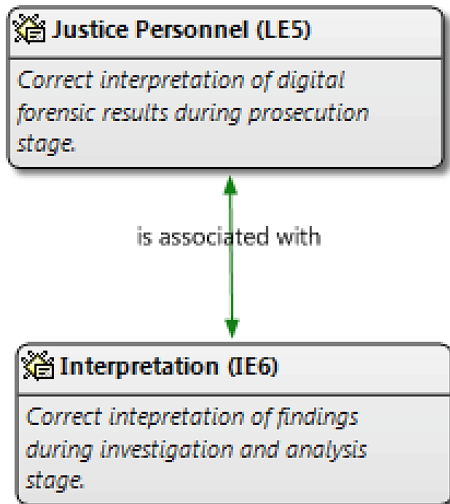


Figure 18: Analysis of the Justice System Implementation system.

The above finding demonstrates the shared *common purpose* of components LE5 and IE6. The self-assessment results show that the requirements of this system were fully met. Therefore, a *full compliance* rating was noted against this system.

**7.3.3.3 e-Crime Prosecution System (LE4 to IE8)**

Findings from an analysis of this system show that Law Enforcement Agents (LE4) met the requirements set out by the component (IE8), as required by the model, by demonstrating knowledge and willingness to investigate during the execution of the Anton Piller order. Further, they acted in *accordance with* industry requirements by providing written testimony on the process followed, and detailing their findings (see Figure 21).

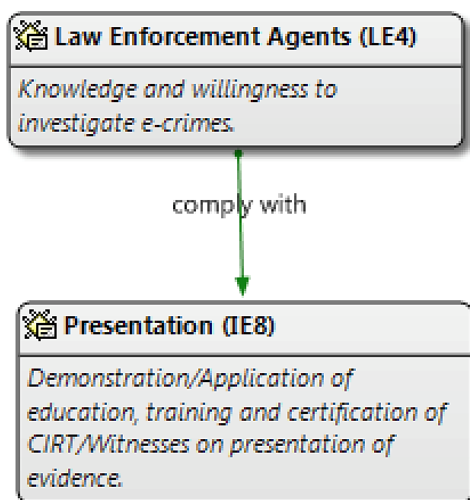


Figure 19: Analysis of the e-Crime Prosecution system.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

Therefore, the results of the self-assessment show that all components were found to exist, as per the model, and thus a *full compliance* rating was allocated.

### 7.3.3.4 Evidence Handling System (CE4, LE3 and IE2)

Findings show that correct interdependencies existed between CE4 and LE3, in that representatives of the company could cooperate with the justice system by presenting sufficient evidence to support their claim that an ex-employee could be responsible for the defamatory email which was sent to the company's staff, competitors and customer database. It is this cooperation which led to the court granting the Anton Piller order. As a result, a *full compliance* rating was allocated against the implementation of CE4 and LE3.

Additionally, those representing the Justice System (LE3) were able to detail limitations of scope in the Anton Piller order, thereby restricting the collection of evidence (IE2) to only those items that were specific to proving that the ex-employee was the author of the disputed email. See Figure 22. As a result, a *full compliance* rating was allocated against the implementation of LE3 and IE2.

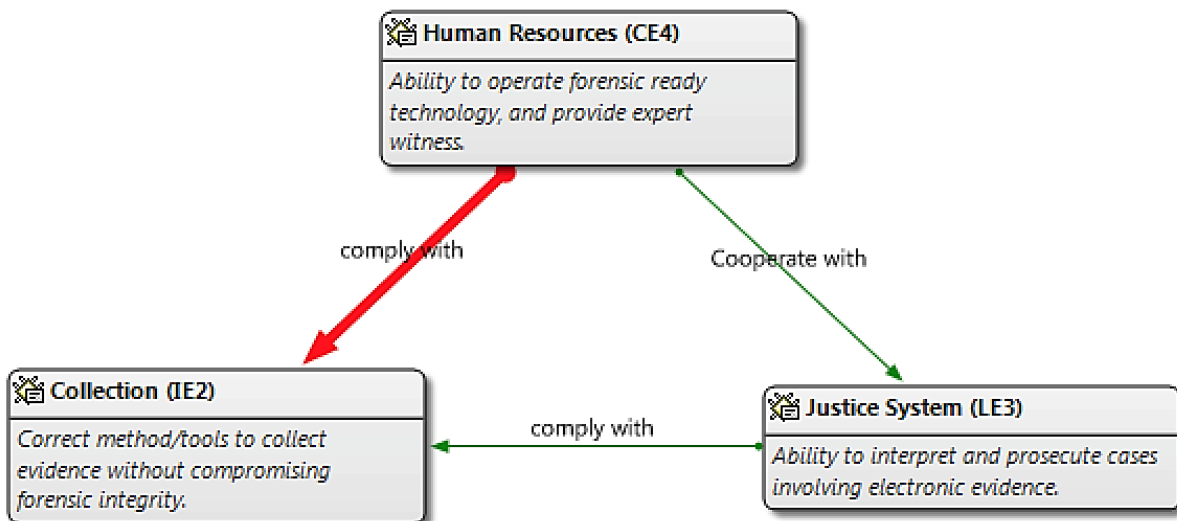


Figure 20: Analysis of the Evidence Handling system.

The self-assessment identified *partial compliance* in the nature of the dependency between Human Resources (CE4) and Collection (IE2). This partial compliance refers to the finding that while correct methods and tools were used to collect evidence, some of the evidence collected was out of scope and not in agreement with what the court order had stipulated.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**7.3.3.5 Standards Localisation System (IE8, CE1 and LE1)**

A *full compliance* rating was allocated against the implementation of components CE1 and LE1, and components IE8 and CE1, respectively. This is because the organisation was able to convince (IE8) the courts that it is one of a handful of companies in the logistics industry, with specific standards (CE1) of operation, including the use of sophisticated software to facilitate warehousing and distribution. Further that all the above were compliant with electronic laws (LE1) (see Figure 23).

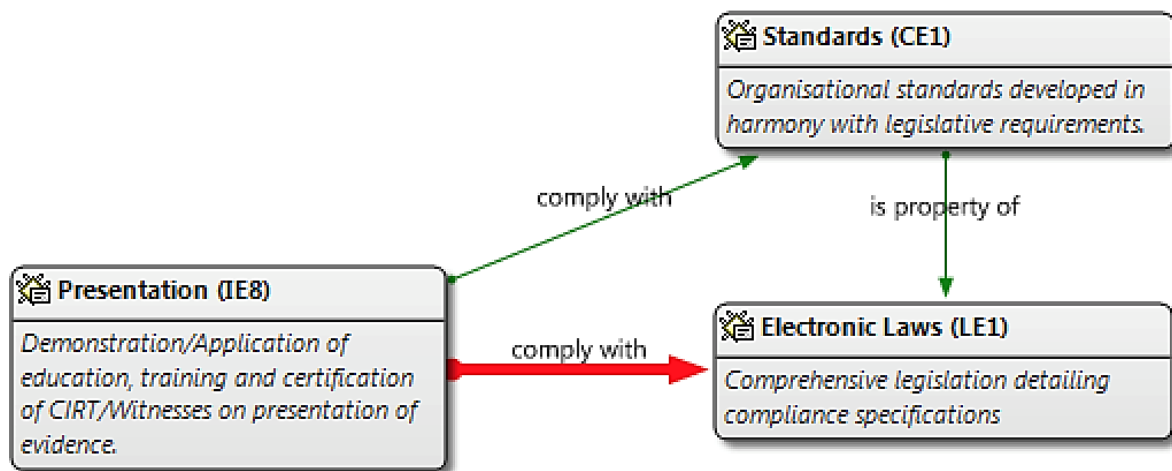


Figure 21: Analysis of the Standards Localisation system.

However, findings show that the vulnerability was that the evidence led in testimony (IE8) was incomplete. This evidence did not meet the requirements of the law (LE1) in that some evidence led was out of scope, and those giving testimony did not fully disclose all relevant case facts to the court. Therefore, the nature of the relationship between IE8 and LE1 is noted in the self-assessment as being *partially* compliant.

**7.3.3.6 Policy Alignment System (CE2, IE8 and LE1)**

As with the Standards Localisation system, the organisation was able to demonstrate to the courts that it operates in a niche industry. As such it has written policies (CE2), which govern the behaviour of those interacting with the organisation, to protect itself from incidents stemming from within, or outside, the organisation. Included in these policies are those that protect the organisation against the use of its own intellectual property for malicious purposes. Further, that said policies are in accordance with the law (LE1). Thus, a *full compliance* rating was allocated for the interdependency between CE2 and LE1, and a further *full compliance*

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

granted for the interdependency between components CE2 and IE8 (see Figure 24).

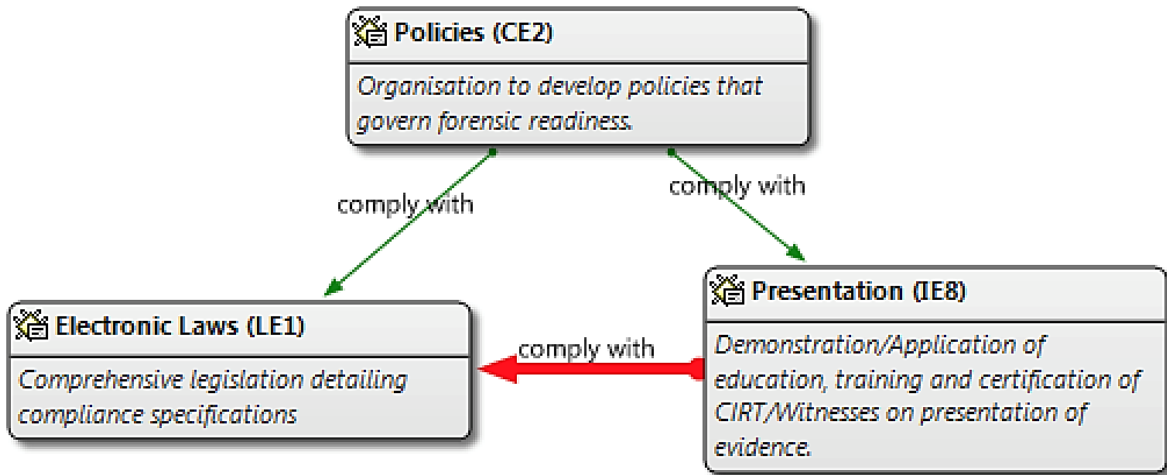


Figure 22: Analysis of the Policy Alignment system.

While the self-assessment identified correct interdependencies to exist between components, as discussed previously, the nature of the relationship between Presentation (IE8) and Electronic Laws (LE1) was found to be vulnerable. This vulnerability was found to be a result of *partial* compliance of evidence led in testimony (IE8) as it did not meet the requirements of the law (LE1) in that some of the evidence was out of scope and those giving testimony did not fully disclose all relevant case facts to the court.

### 7.3.3.7 Witness Preparation System (CE4, IE8 and LE2)

In this case, the self-assessment identified *partial* compliance in the nature of the dependency between all components of the system. This partial compliance refers to the finding that the organisation's representatives (CE4) failed to present the court with all the facts relating to the case, that the witness testimony (IE8) was partly based on evidence which fell outside the scope of the court order (LE2), thereby causing the court to rule that the Anton Piller order was not executed in accordance with the law (see Figure 25).

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

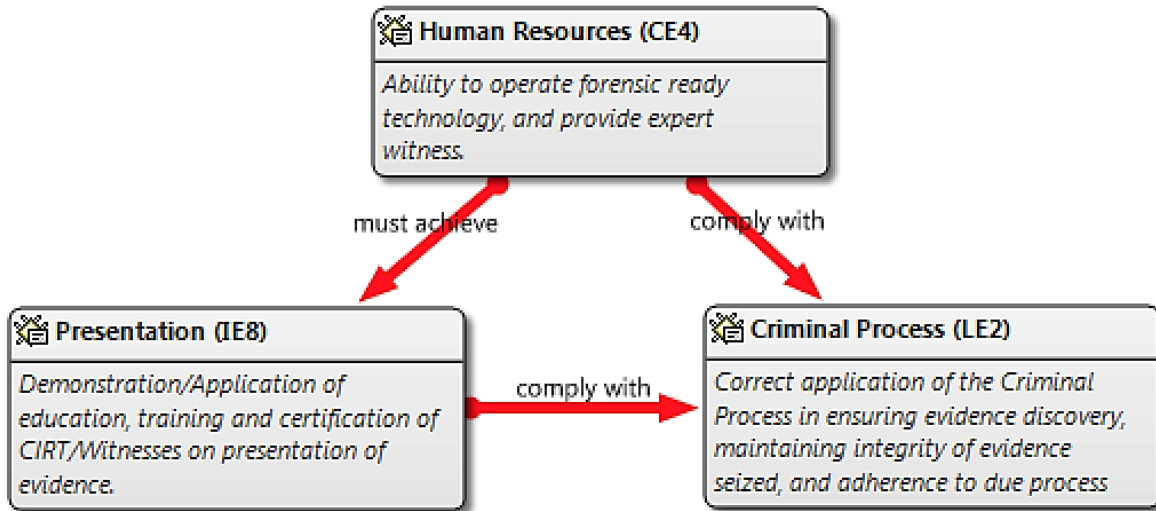


Figure 23: Analysis of the Witness Preparation system.

**7.3.3.8 Procedural Implementation System (CE3, LE2 and IE8)**

Findings show that all components of the system were found to exist and that the interdependencies between components CE3 and LE2 were as defined by the model. The organisation was able to follow correct internal procedures in preparing a compelling case for the court to grant an Anton Piller order, *in accordance with* the Criminal Process (LE2). For this reason, a *full compliance* rating was allocated during self-assessment (see Figure 26).

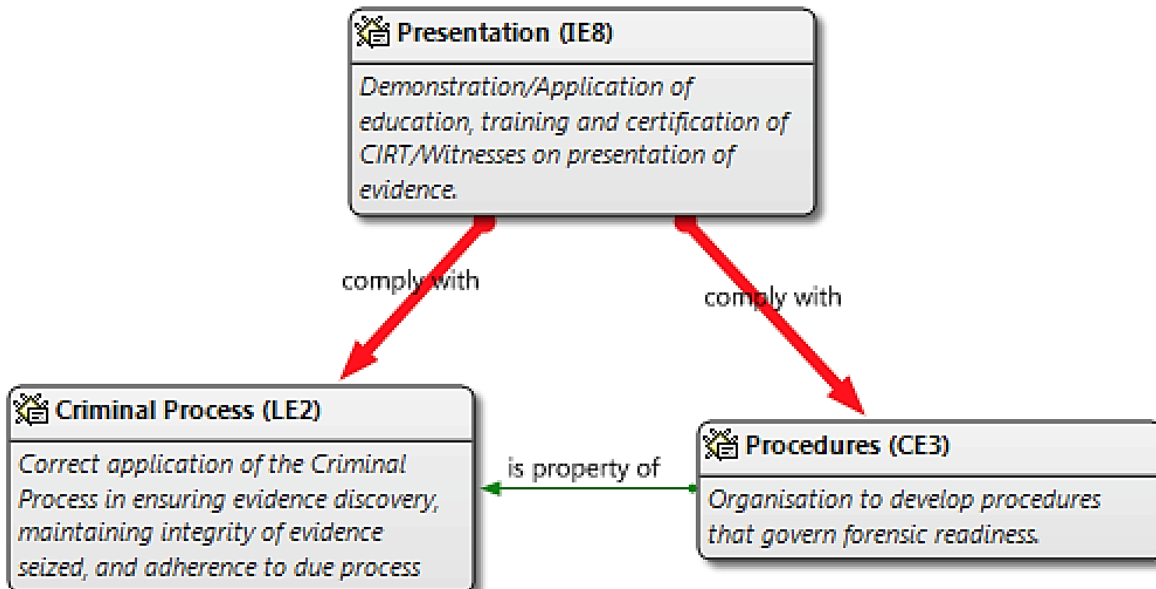


Figure 24: Analysis of the Procedural Implementation system.

However, while the model identified correct interdependencies between components CE3 and



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

LE2, vulnerabilities were found in how IE8 interacts with LE2 and CE3, respectively. These vulnerabilities relate to the *partial* compliance noted during the self-assessment stage. The *partial compliance* was the result of findings which show that evidence led in testimony (IE8) failed to comply with the requirements of the law (LE2) and organisational procedures (CE3) in that it was incomplete and partly based on incorrect evidence.

**7.3.3.9 Evidence Preservation System (CE5, IE1 and LE2)**

An analysis of this system shows that the organisation could demonstrate to the court that they make use of sophisticated and legal industry specific software which facilitates operations in this niche logistics environment. This convinced the courts that the author of the email in question was someone from within the industry, and most likely the organisation itself. As a result, an Anton Piller order was granted by the court. Therefore, a *fully compliant* rating was granted in the self-assessment for the interdependencies between CE5 and LE2 (see Figure 27).

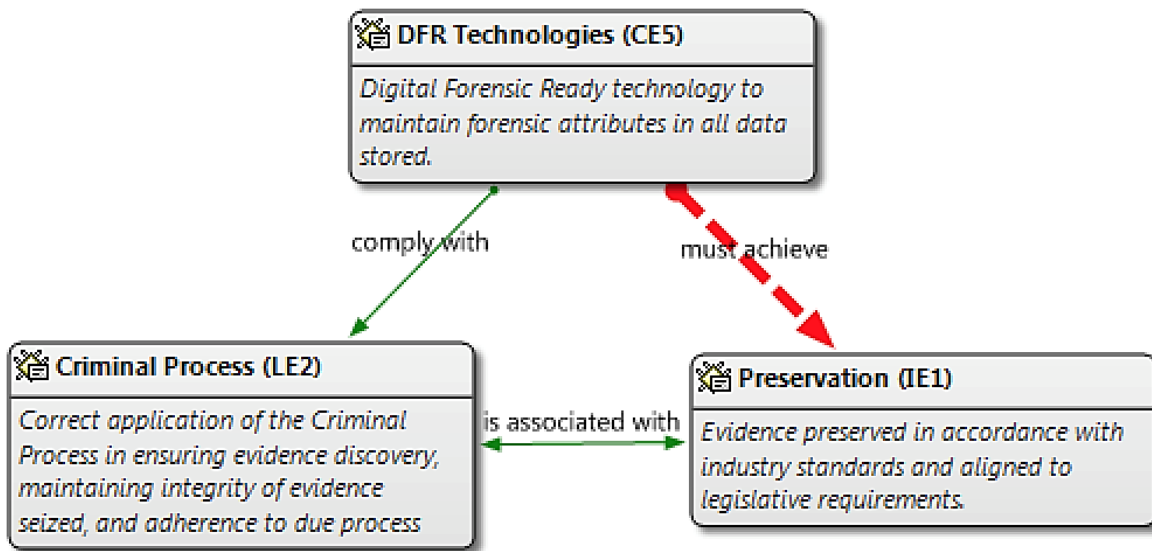


Figure 25: Analysis of the Evidence Preservation system.

In addition, the organisation could demonstrate to the court that they applied correct industry processes in preserving evidence and that the integrity of such evidence was maintained, as per the criminal process. As a result, the court accepted the validity of the evidence preservation process. For this reason, a *full compliance* rating was granted on the interdependency between LE2 and IE1.

Finally, findings show a vulnerability between CE5 and IE1 which, in the self-assessment, is noted as a total *noncompliance* to the requirements of the model. Findings show that DFR

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

Technologies failed to prevent and identify *if* and *how* company intellectual property could have been taken by the then Chief Information Officer, or any other disgruntled employee, and end up in the hands of customers in the form of the disputed email. While preliminary evidence was sufficient for the court to grant an Anton Piller order, the organisation failed to gather sufficient evidence to support their claims, resulting in the court dismissing the case.

### 7.3.3.10 Methodology Evaluation

An analysis of the Methodology Evaluation system shows that those representing the justice system were able to interpret findings from the application of the digital forensic methodology used in the execution of the Anton Piller order. A *full compliance* rating was granted for the interdependencies between components LE3 and IE2. This was due to LE3's ability to identify that correct methods and tools had been used to collect evidence, that the integrity of said evidence was maintained and that it could be tested in a court of law (see Figure 28).

Additionally, a *full compliance* rating was granted for the interactions between components LE3 and IE9. The latter is because the court stipulated the conditions under which evidence was to be retained during the execution of the Anton Piller order and, upon dismissing the case, ordered for such evidence to be returned to its rightful owners.

The self-assessment identified a further seven cases of *partial compliance* relating to components IE1 and IE3 to IE8. This was as a result of the court ascertaining that some of the evidence presented fell *outside* the scope of the court order. This resulted in the preservation, validation, identification, analysis, interpretation documentation and presentation of evidence outside the scope of the Anton Piller order. Additionally, the court found gross inefficiencies in the submitted documentation which was intended to itemise evidence inventory. This documentation was found to lack the necessary detail to validate the contents of the evidence bags. This suggests that those representing the justice system were sufficiently able to interpret and prosecute the case in question (see Figure 28).

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

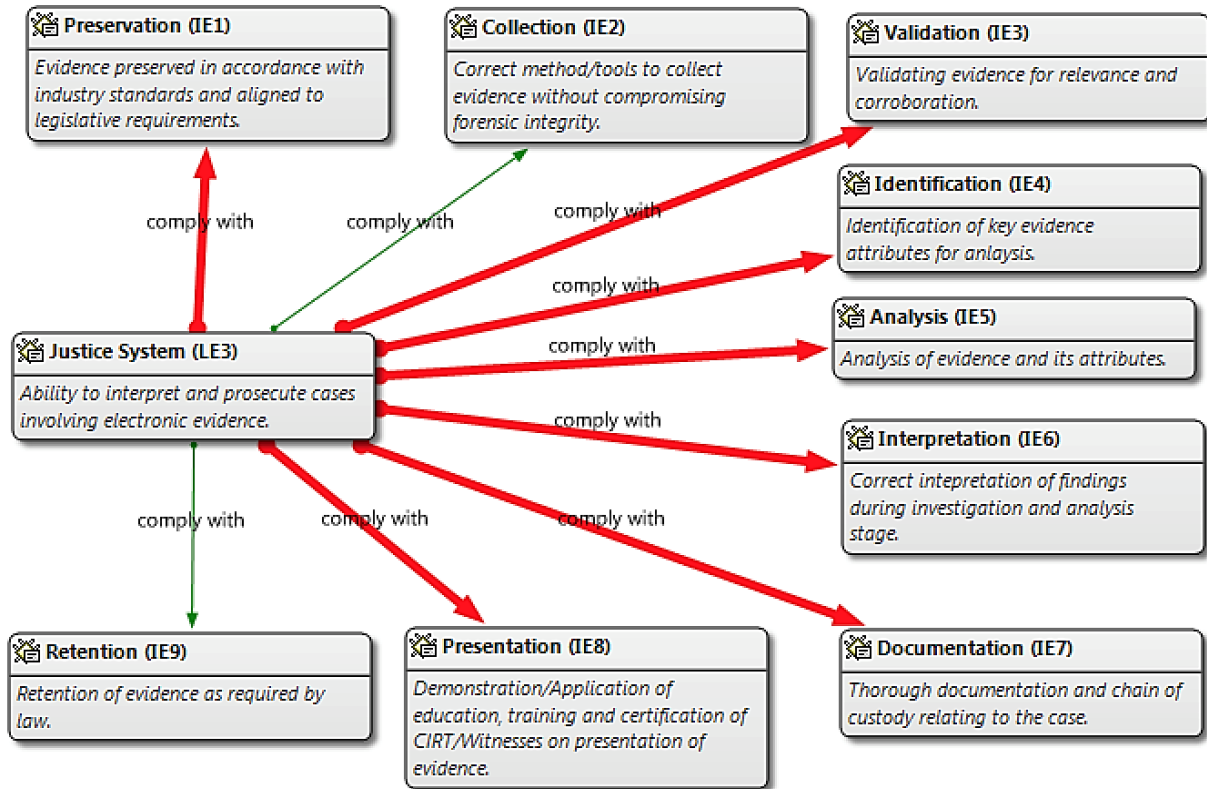


Figure 26: Analysis of the Methodology Evaluation system.

The process identified system interdependency issues relating to the evidence preservation system. This suggests that the nature of the interdependency between components CE5 and IE1 is not in accordance to what the M-DiFoRe model proposes. This is the only system which was found to be noncompliant with the M-DiFoRe model. Further findings show six systems with instances of partial compliance, and a further three systems that have full compliance with the M-DiFoRe model. The final step to implementing the gap analysis deals with the process to follow in order to remediate noncompliant and partially compliant systems, with the objective of advancing them to a fully compliant state. This is discussed later in this chapter.

The next section compares results from having applied steps 1 to 3 of the self-assessment, and those from the qualitative analysis.

### 7.3.4 Activity 4 - Results Comparison

When comparing the results of the self-assessment in section 7.3.2 (Appendix 9) with the results from the qualitative analysis in section 7.3.3 (Figure 18) it is clear that the degree of similarity is total. With both methods (Appendix 9 and Figure 18), it was possible to identify the one system that was **noncompliant**, the six **partially compliant** systems and the three fully

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

compliant systems. Table 23 provides a brief observation on the specific component pairs which were found to be noncompliant and partial compliant, respectively.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

<b>System</b>	<b>Activity 2 – Self Assessment (section 7.3.2.3)</b>	<b>Activity 3 – Qualitative Analysis (section 7.3.3)</b>	<b>Observation</b>
<b>Noncompliance</b>			
Evidence Preservation (IE8, CE3, LE2)	CE5, IE1	CE5, IE1	DFR technology failed to preserve the required evidence thereby failing to identify <i>if</i> and <i>how</i> intellectual property could have been taken by the then Chief Information Officer.
<b>Partial Compliance</b>			
Evidence Handling (CE4, LE3, IE2)	CE4, IE2	CE4, IE2	Improper collection of evidence due to some of the evidence being collected being out of scope and not in agreement with what the court order had stipulated,
Standards Localisation (IE8, CE1, LE1)	IE8, LE1	IE8, LE1	Failure to disclose all facts relating to office operations as they relate to the then Chief Information Officer’s true role.
Policy Alignment (CE2, IE8, LE1)	IE8, LE1	IE8, LE1	Failure to disclose all facts relating to office operations as they relate to the then Chief Information Officer’s true role.
Witness Preparation (CE4, IE8, LE2)	CE4, LE2	CE4, LE2	Insufficient evidence during criminal proceedings. Role of the then Chief Information Officer in relation to the alleged Christmas list could not be clearly proven.
	CE4, IE8	CE4, IE8	Employees led evidence outside scope of court order.
	IE8, LE2	IE8, LE2	Failure to comply with criminal process in that the Anton Piller order was not executed as prescribed by the court.
Procedural Implementation (IE8, CE3, LE2)	IE8, CE3	IE8, CE3	Testimony led by employees was found to be inconsistent with organisational procedures. Staff alleged that the then Chief Information Officer was party to certain procedures, which the court found untrue.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

	IE8, LE2	IE8, LE2	Failure to comply with criminal process in that the Anton Piller order was not executed as prescribed by the court.
Methodology Evaluation (LE3, IE1-IE9)	LE3, IE1	LE3, IE1	Inefficiencies in evidence preservation, as some evidence was found to be out of scope.
	LE3, IE3	LE3, IE3	Inefficiencies in evidence validation, as some evidence was found to be out of scope.
	LE3, IE4	LE3, IE4	Inefficiencies in evidence identification, as some evidence was found to be out of scope.
	LE3, IE5	LE3, IE5	Inefficiencies in evidence analysis, as some evidence was found to be out of scope.
	LE3, IE6	LE3, IE6	Inefficiencies in interpretation of evidence, as some evidence was found to be out of scope.
	LE3, IE7	LE3, IE7	Inefficiencies in evidence documentation, as the inventory lists prepared were incomplete.
	LE3, IE8	LE3, IE8	Inefficiencies in evidence presentation, as some evidence was found to be out of scope.

Table 23: Comparison of self-assessment results to qualitative analysis.

This confirms the validity of the model as it identified the same vulnerabilities.

With the vulnerabilities now determined, the next step in applying the M-DiFoRe model is to undertake remedial action on vulnerable systems, to bring the affected systems into full compliance with the requirements of the model. This is discussed next.

### 7.3.5 Activity 5 – (Step 4) Remedial Action

The final step in applying the model is to take corrective measures to bring vulnerable systems into a fully compliant state. This process is non-linear and thus allows the organisation to implement the model starting at any layer, based on priorities identified in the self-assessment.

As discussed in section 6.4.2.2, the M-DiFoRe model provides guidelines as to the ideal nature

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

of system interdependencies. Applying remedial action to vulnerable systems requires that an organisation base their corrective measures on model guidelines, as referenced under step 4 in Appendix 9. The numbers in the Reference column refer to the paragraph numbers in Chapter 6 which relate to the specific system. Table 24 provides a summary of the recommended remedial action to be taken on vulnerable systems.

System	Activity 2 – Self Assessment (section 7.3.2.3)	Remedial Action description	Reference
<b>Noncompliance</b>			
Evidence Preservation (IE8, CE3, LE2)	CE5, IE1	Correct implementation and configuration of DFR technologies, including event logging.	6.3.3.2(vi)
<b>Partial Compliance</b>			
Evidence Handling (CE4, LE3, IE2)	CE4, IE2	Strict adherence to court order on evidence to be collected.	6.3.3.2(i)
Standards Localisation (IE8, CE1, LE1)	IE8, LE1	Present evidence that is within scope of court order. Full disclosure of facts.	6.3.3.2(ii)
Policy Alignment (CE2, IE8, LE1)	IE8, LE1	Present evidence that is within scope of court order. Full disclosure of facts.	6.3.3.2(ii)
Witness Preparation (CE4, IE8, LE2)	CE4, LE2	Employees to present all facts to the court.	6.3.3.2(iv)
	CE4, IE8	Testimony given to court to be based on evidence within scope of court order.	6.3.3.2(iv)
	IE8, LE2	Testimony to demonstrate compliance with the criminal process.	6.3.3.2(v)
Procedural Implementation (IE8, CE3, LE2)	IE8, CE3	Testimony to demonstrate compliance with organisational procedures.	6.3.3.2(v)
	IE8, LE2	Testimony to demonstrate compliance with the criminal process.	6.3.3.2(v)
	LE3, IE1	Preservation of correct evidence using correct process.	6.3.3.3

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Methodology Evaluation (LE3, IE1-IE9)	LE3, IE3	Adherence to rules of evidence validation.	6.3.3.3
	LE3, IE4	Adherence to rules of evidence identification.	6.3.3.3
	LE3, IE5	Analysis of data that falls within scope of court order	6.3.3.3
	LE3, IE6	Correct interpretation of evidence.	6.3.3.3
	LE3, IE7	Maintaining proper chain of evidence.	6.3.3.3
	LE3, IE8	Presentation of evidence that falls within scope of the court order.	6.3.3.3

Table 24: Recommended remedial action on vulnerable systems

The following section provides a detailed discussion of the individual remedial actions that should have been taken to avoid the evidentiary data being negated.

### 7.3.5.1 Recommended remedial action on noncompliant systems

Further findings show that the self-assessment process identified one system, namely Evidence Preservation, that had a **noncompliant** rating.

As discussed earlier, noncompliant ratings present the highest risk to the organisation and should be treated as a priority when implementing the model. In the case law discussed, findings show that the noncompliant system ultimately led to the dismissal of the case by the court. As per references provided to support the noncompliant finding, the organisation failed to identify *if* and *how* intellectual property could have been taken by the then Chief Information Officer (CIO), or any other disgruntled employee. This intellectual property then ultimately ended up in the hands of customers, in the form of the disputed email.

The recommendation, as per section 6.3.3.2(vi), is thus for the organisation to ensure correct implementation and configuration of DFR technologies, including event logging. In this case, the organisation should have implemented DFR technology to log user activities and manage access control to critical files and applications. In doing this the organisation would have been able to present accurate information to the court in respect to whether, or not, the then Chief Information Officer had any access to the alleged intellectual property, referred to



## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

as the “Christmas list” in the case, and his role in the distribution thereof, including his participation in the defamatory email.

### 7.3.5.2 Recommended remedial action on partially compliant systems

According to the results of the self-assessment, six of the systems evaluated had vulnerabilities that were rated as partially compliant. These systems, as identified by their **partially compliant** status (column 8 of Appendix 9) and the recommended action (column 10 of Appendix 9) are:

- i. Evidence Collection: remedial action is to ensure strict adherence to court order regarding evidence to be collected. Adherence to the court order would have ensured that only evidence which fell within the ambit of the order was collected. The supervising attorneys should have monitored the process closely to ensure that evidence collected was as defined in the court order.
- ii. Standards Localisation: remedial action is for employees to present all facts during testimony. Employees were to ensure full disclosure of facts to the court, so as to enhance the credibility of their testimony. The organisation should have ensured that employees leading evidence received adequate training regarding organisational standards to thus provide factual disclosure of facts relating to the operations of the organisation in relation to roles and responsibilities.
- iii. Policy Alignment: remedial action is for employees to present all facts during testimony. Employees were to ensure full disclosure of facts to the court, so as to enhance the credibility of their testimony. The organisation should have ensured that employees leading evidence received adequate training concerning organisational policy to thus provide factual disclosure of facts relating to the operations of the organisation.
- iv. Witness Preparation: remedial action is for employees to be prepared and encouraged to present all facts to the court (full disclosure), and to provide testimony based on evidence that is within the scope of the court order. The latter, together with ensuring full compliance with the criminal process, would have placed employees in a position where they could have demonstrated competence and credibility to the court.
- v. Procedural Implementation: remedial action is for employees giving testimony to be prepared to demonstrate compliance with organisational procedures and the criminal process. Offering the required preparatory training to employees would have eliminated inefficiencies relating to evidence collection and would have enhanced their credibility.
- vi. Methodology Evaluation: remedial action is to ensure proper application of the digital

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

forensic methodology. The supervising attorney should have communicated the court's expectations to the technical team so that their activities could have been aligned with all the requirements of the court order. This would have given the court comfort in the credibility of the process followed.

Further findings show that the *partial compliance* found in the case analysed, refers to human error which would have been impossible to identify had the self-assessment been conducted *pre* the court case. This suggests that in evaluating systems vulnerable to human error, the questions asked need to include those that seek to establish *what has been done to ensure strict compliance to those aspects of the system which are susceptible to human error*.

### 7.4 Conclusion

The goal of this chapter was to *validate the interdependencies* between the proposed model's *systems* using a case which the court had judged inadmissible. The validation process was conducted through the analysis of the case law, as presented in the South African courts.

As per the synopses presented, the case law refers to an incident that took place in 2010, wherein the applicants alleged that the respondent had sent a *defamatory email* to its customers, competitors and staff. The email also severed contractual relationships.

This chapter continued with the exploration of evidence to suggest that the proposed model is *sufficiently accurate for its intended use* of enabling organisations to reduce the potential dangers from the inadvertent destruction and negating of evidentiary data and to improve their overall organisational digital forensic readiness. This was achieved through the following five key activities:

- i. Activity 1 - Present case law synopsis where electronic evidence was found inadmissible;
- ii. Activity 2 - Apply steps 1 to 3 of the self-assessment template to said case law;
- iii. Activity 3 - Perform a qualitative analysis on said case law;
- iv. Activity 4 - Compare results from activities ii and iii above and
- v. Activity 5 - Apply step 4 of the self-assessment template to said case law.

Findings show that:

- i. The self-assessment (as presented in Appendix 9) served as an *effective tool* to identify

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

(Activity 2) and provide remedial action (Activity 5) on vulnerabilities in the case analysed. Had the model been applied, it could have *mitigated* the risk of inadvertently destroying and negating evidentiary data.

- ii. The comparison of results obtained through the self-assessment process in section 7.3.2 (Appendix 9) with those from the qualitative analysis in section 7.3.3 (Figure 18) show a complete degree of similarity, which validates the M-DiFoRe model.

Based on these finding, the M-DiFoRe model can be considered *sufficiently accurate for its intended use* of enabling organisations to reduce the potential dangers from the inadvertent destruction and negating of evidentiary data and improving overall organisational digital forensic readiness.

The M-DiFoRe model, as illustrated in Figure 18, is therefore presented as the final model without any changes.

## **8. Chapter 8: Conclusion**

---

### **8.1 Introduction**

As discussed in the introductory section of Chapter 1, most countries recognise the importance of the criminalisation of malicious computer related acts to promote a secure business environment. However, literature review findings in section 1.2 suggest that few countries possess the legal and technical resources necessary to address the complexities of adapting criminal statutes to cyberspace. The proposed solution, per the literature review, is a coordinated, public-private partnership to produce a model approach which can help eliminate the challenges faced by developing countries.

It is against this backdrop that the study explored the development of a multidisciplinary digital forensic model for use in developing economies, utilising the South African legal context as a reference point.

As presented in the problem statement (Chapter 1, section 1.3), this study undertook to develop and assess a digital forensic readiness model using a coordinated, multidisciplinary approach involving both the public and private sectors, with the aim of enabling organisations to reduce the potential dangers from the inadvertent destruction and negating of evidentiary data. To achieve this, a set of 10 hypotheses were created (See Chapter 1, section 1.5). Each of these was linked to five research objectives which emerged during the preliminary literature survey as challenges faced by corporations, and countries at large, when dealing with digital crimes. Table 1 presents a summary linking each of the literature themes to the 10 hypotheses (as discussed in Chapters 2 and 4).

This study comprised 8 chapters, each with a specific goal contributing towards the purpose statement (section 1.6). The purpose statement sought to develop, and explain, how a model based, multidisciplinary approach to digital forensic readiness can aid in preserving the integrity of evidentiary data within an organisation.

The next section summarises the content of the chapters of this study.

### **8.2 Chapter Summary**

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

Below is a synopsis of each chapter's goal, the research process adopted and overall findings.

### 8.2.1 Chapter 1: Introduction

The goal of this introductory chapter was to contextualise the research which detailed the problem statement, the paradigm and methodological choices made for this research (see section 1.7).

To explore the problem statement, the study used 10 hypotheses, each linked to a research objective. Table 1 lists the hypotheses and their corresponding research objectives. This chapter also employed a literature survey to motivate the study and to demonstrate that the problem statement presents a real problem to be solved.

### 8.2.2 Chapter 2: Systematic Literature Review

The goal of this chapter was to present a systematic literature review, applied with the purpose of investigating the five hypotheses presented in the chapter.

The said research question was answered by means of five hypotheses which, as per Table 1, relate to each of the five research objectives of this study. See section 2.4 for detailed findings.

- i. Hypothesis 1 states that: *electronic evidence gathered during a digital forensic investigation does not provide sufficient assurance of non-manipulation to the courts.* Findings show that existing digital investigation methodologies (Live and Dead forensic acquisition processes) do not provide sufficient assurance of non-manipulation of evidence. The study found that this is due to the rapid changes/advances in storage technologies.
- ii. Hypothesis 2 states that: *there is a lack of standardisation in the criteria against which electronic evidence is validated as no consistent digital forensic methodology exists.* Findings show that the digital forensic industry lacks standardisation in the criteria used for collecting evidence. This has led to a lack of synergy in innovation, as well as limited regulation and misalignment of education and certification relating to digital forensics. This is as a result of various legal systems, which have varying requirements.
- iii. Hypothesis 3 states that: *forensic technology for gathering digital evidence is increasingly lagging behind the advances made in anti-forensic tools and the rapid changes in storage technology.* Findings show that a trade-off in the functionality of information security and digital forensic tools exists. Additionally, that forensic

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

technology for gathering evidence is increasingly lagging behind due to the rapid advances in anti-forensics and changes in technology.

- iv. Hypothesis 4 states that: *individuals involved in the digital forensic investigation and prosecution process are not sufficiently trained and/or educated*. Findings show that those involved in the digital forensic process are not adequately trained and educated, thereby contributing to the inadvertent destruction of evidentiary data.
- v. Hypothesis 5 states that: *an organisation responding to a digital crime, without an incident response plan, may take actions that compromise the admissibility of evidence to a court of law*. Findings show that a mature technical environment is not the only factor impacting on the organisation's digital forensic readiness, and that without an incident response plan, an organisation will take actions that compromise the admissibility of evidence. In addition, the study found that existing literature does not sufficiently define the concept of *digital forensic readiness* for it to be implemented, and that suggestions as to a framework to guide its implementation, are also absent.

With all the hypotheses proven true, this chapter concludes that a need to revisit the underlying principles of digital forensics exists. This provides further evidence of the need for a multidisciplinary digital forensic model, geared particularly towards addressing challenges faced by law enforcement and corporations in developing economies.

### **8.2.3 Chapter 3: Research Design**

The goal of this chapter was to present the design, methodology, and methods adopted in this research.

### **8.2.4 Chapter 4: Data Gathering And Analysis**

The goal of this chapter was to collect interview data from industry experts, to validate findings from the literature survey (Chapter 2) and to investigate the five related hypotheses.

In preparing the research instrument, three questions were formulated to test each of the five hypotheses. The hypotheses were also linked to each of the core literature themes, as discussed earlier. Therefore, the interview process was based on a total of 15 key questions.

Below are the five hypotheses that were investigated in this chapter, and their respective findings (see section 4.4):

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

- i. Hypothesis 6 states that: *as a result of the presence of the electronic laws in South Africa, the prosecution of digital crimes faces no limitations*. Findings suggest that the hypothesis is not true, as a lack of processes, procedures, education, training and certification can serve as limitations during the prosecution of digital crimes.
- ii. Hypothesis 7 states that: *South Africa has a standardised digital forensic model and process that is used by authorities to investigate and prosecute digital crimes*. Findings suggest that this hypothesis is not true, as no single common model or process is in place for the South African legal context.
- iii. Hypothesis 8 states that: *The Electronic Communications and Transactions (ECT) Act of South Africa adequately positions the acceptable use of, and extent to which, electronic evidence can be used in a civil or criminal proceeding*. Findings suggest that this hypothesis is true, as the ECT Act makes it possible to present electronic evidence in a court of law.
- iv. Hypothesis 9 states that: *those individuals involved in the prosecution of digital crimes are knowledgeable, adequately trained and professionally certified*. Findings suggest that this hypothesis is not true, as credentials were noted as being a common limitation amongst prosecutors and investigators alike.
- v. Hypothesis 10 states that: *South African organisations do not need to concern themselves with digital forensic readiness, as digital crimes are not commonplace*. This hypothesis was proven untrue as findings point to a prevalence of various types of digital crimes.

With the exception of Hypothesis 8, all other hypotheses were proven untrue. These findings helped to establish that the key stakeholders in a digital forensic investigation originate from three different domains namely: the corporate environment, the industry environment and the legislative environment. Additionally, this chapter presented a set of critical components under each domain, which point to components needed to satisfy the requirements of that domain. See Table 15 for these domains and their respective components.

### **8.2.5 Chapter 5: Foundational Principles Towards Model Development**

The goal of this chapter was to investigate the significance of the three key domains and each of their respective components (*output from Chapter 4*). This data was then used as a foundation towards the development of the proposed model.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

The literature reviewed is based on each of the components, as shown in Table 15.

Findings confirm that the three identified domains are sufficiently representative of the environments from which key stakeholders in the digital forensic process originate. Additionally, that each of the components, as depicted in Table 15, is correctly allocated under each of the three domains.

The identified domains, and their respective components, serve as a basis for further investigation towards the development of the M-DiFoRe model.

### **8.2.6 Chapter 6: Realisation of the Conceptual Model**

The goal of this chapter was to develop the conceptual model through the investigation of the interdependencies which exist between the components of the three domains (Table 15), as discussed previously.

Findings confirmed that the identified domains, and their respective domains (as per Table 15), were sufficiently comprehensive for their intended use. Additionally, the interdependencies between the components were investigated and findings presented in this chapter.

Finally, Chapter 6 presented the M-DiFoRe model (Figure 16). The development of this model using real life case law, ensured that a coordinated and multidisciplinary approach was achieved, as the involvement of all stakeholders in the case law was carefully assessed.

The chapter also discusses in detail the key differentiators of the M-DiFoRe model that sets it apart from previously developed models as discussed in chapter 6, section 6.5.

### **8.2.7 Chapter 7: Model Validation Approach**

The goal of this chapter was to validate the M-DiFoRe model (Figure 16), using a case that the court found the evidentiary data to be inadmissible. This was done to establish if the model was comprehensive enough for its intended use.

Findings show that the self-assessment (Appendix 9) proved useful in identifying systems whose component interdependencies did not comply with those the M-DiFoRe model proposed. More importantly, the results of the self-assessment (Appendix 9) and those from the



## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

qualitative analysis (Figure 17) were found to be congruent, thereby validating the M-DiFoRe model. The said findings led to the adoption of the M-DiFoRe model (Figure 16) as the final version, without any changes.

This chapter also showed how the results obtained from applying the M-DiFoRe model could be used to make recommendations regarding remedial actions to address identified vulnerabilities.

### **8.3 Revisiting the Problem Statement**

The study set out to address the following five research objectives:

- i. Research Objective 1 (RO1): To identify common factors associated with both the technical and legal challenges faced in the prosecution of digital crimes. This was achieved in Chapter 2, section 2.4.1, by presenting traditional and modern approaches to digital forensics, including the evolution of computer forensics. Additionally, the findings were triangulated in Chapter 4, section 4.4.3, with data obtained from interviews with industry experts.
- ii. Research Objective 2 (RO2): To establish whether organisations in the same legal jurisdiction have, and make use of, a standard digital forensics methodology. This was achieved in Chapter 2, section 2.4.2, by presenting literature relating to standardisation in the digital forensic profession. Additionally, the findings were triangulated in Chapter 4, section 4.4.4, with data obtained from interviews with industry experts.
- iii. Research Objective 3 (RO3): To determine the extent to which advances in digital forensics are meeting the demands of the changing legal and technical landscape. This was achieved in Chapter 2, section 2.4.3, by presenting a discussion regarding the impact of recent advances in storage technologies on existing digital forensic processes. Additionally, the findings were triangulated in Chapter 4, section 4.4.5, with data obtained from interviews with industry experts.
- iv. Research Objective 4 (RO4): To investigate critical factors preventing human resources, directly involved in the investigation and prosecution of digital crimes, from functioning effectively. This was achieved in Chapter 2, section 2.4.4, by presenting a discussion on education, training and certification as three distinct concepts. Additionally, the findings were triangulated in Chapter 4, section 4.4.6, with data obtained from interviews with industry experts.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

- v. Research Objective 5 (RO5): To determine whether organisations are taking the necessary steps to proactively manage the rising scourge of digital crimes. This was achieved in Chapter 2, section 2.4.5, by exploring the concept of *forensic readiness* and the factors that have an impact on it. Additionally, the findings were triangulated in Chapter 4, section 4.4.7, with data obtained from interviews with industry experts.

The problem statement, as per section 1.3, states:

*The organisational risk of inadvertently destroying and negating evidentiary data, due to the complexity and multidisciplinary nature of digital crimes, necessitates the development of a digital forensic readiness model using a coordinated, multidisciplinary approach involving both public and private sectors. Current models are context, technology and/or business process specific, and lack the multidisciplinary approach which seeks to investigate inter-discipline interactions.*

The output of this study is the M-DiFoRe model (Figure 16). This model was developed using a coordinated approach which involved a systematic review of existing literature (Chapter 2) and case law (Chapters 6 and 7), and the participation of industry experts from both the public and private sectors (Chapter 4). The M-DiFoRe model (Figure 16) is a practical model which was verified (Chapter 6) and validated (Chapter 7) using case law. The model was found to be sufficiently accurate for its intended use namely enabling organisations to reduce the potential dangers from the inadvertent destruction and negating of evidentiary data as well as improving overall organisational digital forensic readiness.

The M-DiFoRe model differs (Chapter 6, section 6.5) from existing models as it offers a less complicated and streamlined process for achieving digital forensic readiness, through the use of the accompanying self-assessment tool (Table 19). The self-assessment tool was thoroughly tested using case law (Chapter 7, section 7.3.2) and a qualitative analysis process (Chapter 7, section 7.3.3) and was consequently found to be an effective tool to identify vulnerabilities and provide appropriate remedial action based on the M-DiFoRe model guidelines (Chapter 6, section 6.3.3).

It is with the above in mind, that this study considers the said problem statement solved.

### 8.4 Revisiting the Purpose Statement

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

The purpose of this study was to develop and explain how a model based, multidisciplinary approach to digital forensic readiness can aid in preserving the integrity of evidentiary data within an organisation.

In line with the purpose statement, this study presented the M-DiFoRe model (see paragraph 6.4) and explained how a model based, multidisciplinary approach to digital forensic readiness can aid in preserving the integrity of evidentiary data within an organisation. Additionally, Chapter 7 tested the validity of the proposed model through a rigorous process of analysis against case law.

### **8.5 Research Contribution to Body of Knowledge**

This research is considered a meaningful contribution to the digital forensic body of knowledge and to the general research community for the following reasons:

- i. From the evaluation of existing models as per section 2.2.5.1, this study identified challenges with existing models (section 2.2.5.2), and presents ways in which the proposed model overcomes them (section 6.5).
- ii. As detailed in section 2.3, this study identified gaps in current definitions of Digital Forensics, and adopted a definition that speaks to the digital forensic methodology and process.
- iii. As per Table 15, this study presented three domains and their respective components critical to achieving digital forensic readiness. Additionally, this study expounded on the domains and their respective components by detailing the nature of their interdependencies (systems), as discussed in Chapter 6, and presenting the function of each system, thereby simplifying the concept of *digital forensic readiness*. The domains and components in Table 15 attest to the multidisciplinary nature of the digital forensic investigation value chain.
- iv. Finally, this study presents the M-DiFoRe model, which was validated (Chapter 6) and verified (Chapter 7) to assess its usefulness in achieving digital forensic readiness. It further provides a mechanism, the self-assessment template (Table 15), for the identification of vulnerabilities.

### **8.6 Research Limitations**

The following have been identified as limitations relating to this study:

- i. Limitation 1: This study sets the legal context as South Africa. When applied in other

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

countries, one may find variations in legal provisions relating to electronic evidence.

While the above is an inherent limitation of this study, it does not negate the findings as the model does not discuss specific provisions of the law, but points to the requirement *that* relevant legislation be considered when implementing the applicable systems of the M-DiFoRe model.

- ii. Limitation 2: While the model has been verified and validated and found to be sufficiently accurate for its intended use, findings show that an element of *human error* exists. This finding proposes that people are prone to making errors when performing functions, as they relate to digital forensic readiness.

While this finding does not fall within the scope of the model, it does not negate it as The M-DiFoRe model addresses that which *must* be placed in order to achieve digital forensic readiness.

- iii. Limitation 3: The M-DiFoRe model helps organisations identify vulnerabilities through the use of the self-assessment template. However, the model does not provide a means to fix these vulnerabilities.

This limitation falls outside the scope of this research. However, findings show that this does not negate the model, or the self-assessment template provided.

- iv. Limitation 4: The study identifies three main domains to which stakeholders in the digital forensic process could belong. These three domains were selected as the most dominant and this does not suggest that other, less dominant domains, do not exist.

This does not negate the findings of the study as the domains were found to be multidisciplinary in nature and accommodating of the key stakeholders.

- v. Limitation 5: This study investigates the use of the proposed model within the typical corporate environment, and does not focus on a specific industry, or sector.

The above does not negate the model. Findings show that the multidisciplinary nature of the model allows for it to be applied within various environments.

- vi. Limitation 6: Finally, this study acknowledges that the National Integrated Information and Communication Technologies (ICT) Policy White Paper, which was approved by Cabinet on 28 September 2016, intended to set out the framework of *how* government will provide access to modern communications infrastructure and services to facilitate the entry of new players and meaningful participation of all citizens, including those in rural areas (Department of Telecommunications and Postal Services, 2016).

This document was not included in this study as it was released at the end of this research.

## **8.7 Future Research Opportunities**

Each limitation, as discussed previously, presents an opportunity for further research. These opportunities are:

- i. Opportunity 1: Since this study is based on the South African legal system which, as seen from the case law analysed, is a hybrid of civil, common and customary law (the latter is not covered in this study), a research opportunity would be to apply the study to another legal context and observe *how* this affects interdependencies in the model's components and systems.
- ii. Opportunity 2: Since the study only provides components, and does not link these to any best practice or international standards as a way of facilitating the development of said components, and fix vulnerabilities identified from using the self-assessment template, further research can be undertaken into establishing the linkages between components and international best practice, and investigating how vulnerabilities identified by the M-DiFoRe model can be resolved.
- iii. Opportunity 3: Limit the scope of the new study to a specific business type, industry or sector, to thus gain a deeper understanding of the usefulness of the M-DiFoRe model in the specific chosen context.
- iv. Opportunity 4: The application of the M-DiFoRe model could be done programmatically. Technologies such as Artificial Intelligence and eDiscovery applications could be used to automate the implementation of the M-DiFoRe model.

## **8.8 The Research Value**

The inherent value of applying the M-DiFoRe model, as presented in this study, is:

- i. The reduction of technical complexity: the study serves to reduce the complexity of achieving digital forensic readiness by identifying areas of concern (components), their dependencies (systems) and detailing the function or purpose served by each dependency (system). The resulting value is that more organisations will be able to become digitally forensic ready, thereby addressing the challenge of cybercrime.
- ii. The multidisciplinary focus: while the M-DiFoRe model addresses a technical challenge, it was developed using a multidisciplinary approach, thereby rendering it useful in other disciplines. Most of the current models are based on a uni-disciplinary approach, thereby decreasing the practical applicability thereof.
- iii. The use of the mixed data gathering methods: this study provides evidence of the benefits

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

of utilising various data gathering methods in a single research towards achieving theoretical grounding and triangulating findings. This process strengthens the validity of findings and recommendations.

- iv. **Manage insured liability:** As discussed in Chapter 1, the rising scourge of digital crimes affects organisations and countries at large. While this study provides a model that can assist organisations in achieving digital forensic readiness, it can also serve as a proactive tool to aid in the reduction of insurance premiums, and/or assist organisations in meeting minimum requirements to be insured against cyber and other digital related crimes.
- v. **Stakeholder due care:** in a world of increasing legal and compliance requirements, this study provides tools which senior management, directors and executives can use to demonstrate effort towards managing the risk of digital crimes and preventing harm to the organisation. The model's self-assessment template provides a dashboard that leadership can use to gain insight into the organisation's forensic readiness. This has become increasingly important as is evident in Corporate Governance standards.

The next section presents the researcher's reflections on the research undertaken, and discusses lessons learned.

### 8.9 Self-Reflection

As I reflect on my research journey, the following are lessons learned from the analysis of literature and other content generated as part of this study:

- i. Digital forensics is more about *people* than it is about *technology*. The education, training, certification and/or awareness of relevant stakeholders is a key determining factor to the successful prevention, detection and prosecution of digital crimes. This highlights the need for more integrated and multidisciplinary research approaches.
- ii. Public-private partnerships and cooperation are necessary ingredients to overcoming technical, legal and other limitations faced by governments and corporations in the fight against technology related crimes. This highlights the need to institutionalise digital forensic readiness so that it becomes a focused, dedicated and strategic role performed at enterprise level.
- iii. I find the abovementioned lessons to be congruent with the view of Benbasat and Zmud (2003), which states "the complex and imposing challenges associated with IT management, development, and use demand interdisciplinary approaches to their resolution". To this end, the integrated and multidisciplinary research approaches

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

adopted in this study add meaningful contribution to this discipline.

Specific to the scientific research process, the following points have made a profound impression on me:

- i. When conducting research, the researcher needs to guard against the propensity to rely on assumption, but should rather allow the scientific exploratory nature of the process to naturally unfold.
- ii. When founded upon principles of trust, mutual respect and professionalism, the relationship between the student and supervisor can be such that it enables the student to develop as an independent academic identity.
- iii. Whetten (1989) argues that a meaningful theoretical contribution requires an extensions of existing theory that fundamentally change prior understanding of mechanisms by which relationships operate, which might involve developing new concepts or redefining old ones. By following a sound scientific research process, I was able to produce the M-DiFoRe Model, which satisfies the requirements for a meaningful theoretical contribution as per Whetten (1989).

Finally, the process of undertaking this study has benefited me more than merely attaining a doctoral degree and elevating my comprehension of the digital forensic discipline. Additional skills learned include:

- i. An ability to set and manage long-term goals and the discipline to maintain a work-study-life balance;
- ii. The ability to conduct a rigorous and systematic literature review and to critically analyse and formulate substantiated points of view;
- iii. The ability to apply thinking at a strategic, tactical and operational level;
- iv. The ability to scientifically articulate thoughts and
- v. The ability to create new knowledge, and to critically challenge my own ideas.

I am thankful for the opportunity afforded to me to have embarked on this research journey.

Finally, I consider this research to have been a success, as the M-DiFoRe model was validated, verified and found to adequately address the problem statement presented in Chapter 1.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**References**

---

ACFE SA, (2011) *Cyber Forum* [online]. Available from <http://www.acfesa.co.za/cyber-forum/> [Accessed 15<sup>th</sup> May 2012].

Adelstein, F. (2006) *Live forensics: Diagnosing your system without killing it first*. *Communications of the ACM* [online]. Available from <http://dl.acm.org/citation.cfm?id=1113070&dl=ACM&coll=DL&CFID=672738615&CFTOKEN=59308299> [Accessed 11<sup>th</sup> April 2013].

Armitage, A. (2007) *Mutual Research Designs: Redefining Mixed Methods Research Design* [online]. Available from [www.ethiopia-ed.net/images/1602209283.doc](http://www.ethiopia-ed.net/images/1602209283.doc) [Accessed 6<sup>th</sup> June 2013].

ATLAS.ti. (2011) *Scientific Software Development, A world of data in your hand* [online]. Available from: [www. http://atlasti.com/product/](http://atlasti.com/product/) [Accessed 19<sup>th</sup> March 2012].

Benbasat, I. and Zmud, R. 2003, 'The identity crisis within the IS discipline: defining and communicating the discipline's core properties', *MIS Quarterly*, vol. 27, no. 2, pp. 183–94.

Baryamureeba, V. and Tushabe, F. (2004) *The Enhanced Digital Investigation Process Model* [online]. Available from [http://www.dfrws.org/2004/day1/Tushabe\\_EIDIP.pdf](http://www.dfrws.org/2004/day1/Tushabe_EIDIP.pdf) [Accessed 2<sup>nd</sup> March 2010].

Beaudry, J. S. and Miller, L. (2016) *Research Literacy: A Primer for Understanding and Using Research*. New York: The Guilford Press.

Beebe, N.L. and Clark, J.G. (2005). A Hierarchical, Objectives-Based Framework for the Digital Investigations Process. In: *Digital Investigation*, 2(2), pp. 147–167.

Bell, G. and Boddington, R. (2010) *Solid state drives: The beginning of the end for current practice in digital forensic recovery* [online]. Available from [http://researchrepository.murdoch.edu.au/3714/1/solid\\_state\\_drives.pdf](http://researchrepository.murdoch.edu.au/3714/1/solid_state_drives.pdf) [Accessed 15<sup>th</sup> June 2011].



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Ben-Gera, M. (2009) *Coordination at the centre of government for better policy making paper presented at the Conference on Public Administration Reform and European Integration* [online]. Available from <http://www.oecd.org/site/sigma/publicationsdocuments/42742582.pdf> [Accessed 8<sup>th</sup> October 2013].

Bergmann, M. M. (2011) *The politics, fashions, and conventions of research methods* [online]. Available from <http://mmr.sagepub.com/content/5/2/99.short> [Accessed 6<sup>th</sup> March 2012].

Borkan, J. (1999) Immersion/Crystallization. In: Crabtree, B. F. and Miller, W. L. (eds.) *Doing Qualitative Research*. 2nd ed. California: Sage Publications.

Boyd, N. A. (1998) *Natural Conceptual Modelling Language* [online]. Available from <http://www.educery.com/papers/educer/models/> [Accessed 10<sup>th</sup> December 2016].

Bresnahan, T. and Yin, P. (2007) Standard Setting in Markets: The Browser War. In: Greenstein, S. and Stango, V. (eds.) *Standards and Public Policy*. New York: Cambridge University Press.

Camazine, S., Deneubour, J., Franks, N., Sneyd, J., Theraulaz, G and Bonabeau, E. (2001) *Self-Organization in Biological Systems* [online]. Available from <http://press.princeton.edu/chapters/s7104.pdf> [1<sup>st</sup> September 2013].

Campbell, N. J. (1998) *Writing Effective Policies and Procedures: A Step-by-Step Resource for Clear Communication*. New York: Amacom.

Carrier, B. and Spafford, E. H. (2003) *Getting Physical with the Digital Investigation Process International Journal of Digital Evidence* [online]. Available from [https://www.cerias.purdue.edu/assets/pdf/bibtex\\_archive/2003-29.pdf](https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf) [Accessed 2<sup>nd</sup> March 2010].

Carrier, B. D. (2006) *Risks of live digital forensic analysis* [online]. Available from <http://dl.acm.org/citation.cfm?id=1113069> [Accessed 3<sup>rd</sup> April 2012].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Casasempere, A. (2007) *Making Qualitative Analysis Easy With Basic Content Analysis* [online]. Available from [http://downloads.atlasti.com/library/Casasempere\\_2007-07\\_11.pdf](http://downloads.atlasti.com/library/Casasempere_2007-07_11.pdf) [Accessed 15<sup>th</sup> February 2012].

Casey, E. (2006) *Investigating sophisticated security breaches* [online]. Available from <http://dl.acm.org/citation.cfm?id=1113068&dl=ACM&coll=DL&CFID=672738615&CFTOKEN=59308299> [Accessed 3<sup>rd</sup> April 2012].

Charmaz, K. (2014) *Constructing Grounded Theory* [online]. Available from [https://books.google.co.za/books?hl=en&lr=&id=v\\_GGAwAAQBAJ&oi=fnd&pg=PP1&dq=grounded+theory&ots=YVYzQ7Fym3&sig=ymVKjOipnGijEwfwCwZVzCknN5k#v=onepage&q=grounded%20theory&f=false](https://books.google.co.za/books?hl=en&lr=&id=v_GGAwAAQBAJ&oi=fnd&pg=PP1&dq=grounded+theory&ots=YVYzQ7Fym3&sig=ymVKjOipnGijEwfwCwZVzCknN5k#v=onepage&q=grounded%20theory&f=false) [Accessed 17<sup>th</sup> November 2016].

Chen, F., Koufaty, D. A. and Zhang, X. (2009) *Understanding intrinsic characteristics and system implications of flash memory based solid state drives* [online]. Available from <http://www.cse.ohio-state.edu/hpcs/WWW/HTML/publications/abs09-2.htmlm> [13<sup>th</sup> June 2011].

Contreras, R. (2011) *The Qualitative Data Analysis Software: Making Sense of Research Data* [ATLAS.ti]. Available from: [http://downloads.atlasti.com/library/contreras\\_researchdata.pdf](http://downloads.atlasti.com/library/contreras_researchdata.pdf). [Accessed 9<sup>th</sup> December 2016].

Cook, D. A. and Skinner, J. M (2005) *How to Perform Credible Verification, Validation, and Accreditation for Modelling and Simulation* [online]. Available from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.640.7396&rep=rep1&type=pdf> [Accessed 9<sup>th</sup> December 2016].

Cooper, P., Finley, G. T. and Kaskenpalo, P. (2010) *Towards standards in digital forensics education*, paper presented at the *Proceedings of the 2010 ITiCSE Working Group Reports* [online]. Available from <http://0-delivery.acm.org.oasis.unisa.ac.za/10.1145/1980000/1971688/p87-cooper.pdf?ip=163.200.81.46&id=1971688&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF1D7BC984CB8128A6031F1501F53249B4D&CFID=371942316&CFTOKEN=92269>

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

[657&\\_acm\\_=1382265654\\_8a7f514cedfa67bc30e81d582884acb1](#) [Accessed 5<sup>th</sup> April 2012].

Coopman, R. (2009) *Local Law Enforcement and its Digital Forensics Future* [online]. Available from <http://libcat.post.ca.gov/dbtw-wpd/documents/cc/42-Coopman.pdf> [Accessed 4<sup>th</sup> March 2010].

Corbin, J. M. and Strauss, A. L. (2008) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. California: Sage Publications.

Craig, D.V. (2009) *Action Research Essentials*. California: Jossey-Bass.

Creswell, J. W. and Clark, V. L. P. (2011) *Designing and conducting mixed methods research*. 2<sup>nd</sup> ed. California: Sage Publications.

Crichton, S. and Kinash, S. (2003) *Canadian Journal of Learning and Technology Virtual Ethnography: Interactive Interviewing Online as Method* [online]. Available from <http://www.cjlt.ca/index.php/cjlt/article/view/40/37> [Accessed 12<sup>th</sup> February 2012].

Cross, J. (2006) *Training vs. Education: A Distinction That Makes A Difference* [online]. Available from [http://docs.google.com/viewer?a=v&q=cache:-fqqZWm7YOYJ:internetttime.com/Learning/articles/training.pdf+education+vs+training&hl=en&gl=za&pid=bl&srcid=ADGEESgVDjLXoJ96htH9f23gFBIDDe9uqghQ-rk5z3kY-izzjCylklavoh0JD72cG8\\_44oPKeoy2cw5wOL5x2D5JseXae\\_ABrRlxpDlx-Qt6NuLEkkhodfX8P3RdDeMiipPGyU0pwTKL&sig=AHIEtbQ1zeugD\\_qvbdFhn26Zj8T9wlpJhA](http://docs.google.com/viewer?a=v&q=cache:-fqqZWm7YOYJ:internetttime.com/Learning/articles/training.pdf+education+vs+training&hl=en&gl=za&pid=bl&srcid=ADGEESgVDjLXoJ96htH9f23gFBIDDe9uqghQ-rk5z3kY-izzjCylklavoh0JD72cG8_44oPKeoy2cw5wOL5x2D5JseXae_ABrRlxpDlx-Qt6NuLEkkhodfX8P3RdDeMiipPGyU0pwTKL&sig=AHIEtbQ1zeugD_qvbdFhn26Zj8T9wlpJhA) [Accessed 5<sup>th</sup> April 2010].

Curtis, G. (2012) *The law of cybercrimes and their investigations*. Florida: CRC Press.

Daniel, L. and Daniel, L. (2012) *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom*. MA: Syngress.

David, J. (1999) *Incident response* [online]. Available from <http://www.sciencedirect.com/science/article/pii/S1353485800800057> [Accessed 11<sup>th</sup> April 2012].

Debbabi, M., Hassaine, F., Jarraya, Y., Soeanu, A. and Alawner, L. (2010) *Verification and*

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

*Validation in System Engineering: Assessing*. Springer-Verlag, Heidelberg: *UML/SysML Design Models*.

Delaney, J. T., Lewin, D. and Ichnioswki, C. (1993) *Human Resource Policies and Practices in American Firms*. Darby: Diane Publishing Co.

Department of Telecommunications and Postal Services, (2016) *National Integrated ICT Policy White Paper* [online]. Available from [http://www.dtps.gov.za/images/phocagallery/Popular\\_Topic\\_Pictures/National\\_Integrated\\_ICT\\_Policy\\_White.pdf](http://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National_Integrated_ICT_Policy_White.pdf) [Accessed 30<sup>th</sup> September 2016].

Digital Forensic Research Workshop, (2016) *About Us* [online]. Available from <https://www.dfrws.org> [Accessed 7<sup>th</sup> September 2016].

Doherty, E. and Liebesfeld, J. (2008) *Proposing a digital forensics grange* [online]. Available from <http://0--proquest-umi-.com-.oasis-.unisa-.ac-.za/pqdweb-?did=1480181371-&sid=1-&Fmt=3-&clientId=27625-&RQT=309-&VName=PQD> [Accessed 12<sup>th</sup> May 2013].

Chan, E., Venkataraman, S., David, F., Chaugule, A. and Campbell, R. (2010) *Forenscope: A framework for live forensics. Proceedings of the 26th Annual Computer Security Applications Conference*. [Online]. **26**, p. 307-316. Available from <http://0-dl.acm.org.oasis.unisa.ac.za/citation.cfm?id=1920261.1920307&coll=DL&dl=ACM&ticket=ST-263647-PHrEuXLsz0pJNKsP4ULH-cas> [Accessed 18<sup>th</sup> July 2013].

Elliot, D., Swartz, E. and Herbane, B. (2010) *Business Continuity Management: A Crisis Management Approach*. 2<sup>nd</sup> ed. New York: Routledge.

Elyas, M., Maynard, S.B., Ahmad, A. and Lonie, A. (2014) *Towards A Systemic Framework for Digital Forensic Readiness* [online]. Available from [https://www.researchgate.net/publication/264898131\\_Towards\\_A\\_Systemic\\_Framework\\_for\\_Digital\\_Forensic\\_Readiness](https://www.researchgate.net/publication/264898131_Towards_A_Systemic_Framework_for_Digital_Forensic_Readiness) [Accessed 12<sup>th</sup> October 2016].

Egyedi, T. N. and Blind, K. (2008) General introduction. In: Egyedi, T. N. and Blind, K. (eds.) *The Dynamics of Standards*. Northampton: Edward Elgar Publishing Inc.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Fox, C., Albertson, K. and Wong, K. (2013) *Justice Reinvestment: Can the Criminal Justice System Deliver More for Less?* Oxon: Routledge.

Fox, W. and Bayat, M.S. (2007) *A Guide to Managing Research*. Cape Town: Juta & Co.

Francis, T. (2004) *Commonwealth Law Bulletin Special commemorative edition: 30 years of the CLB* [online]. Available from <http://books.google.com/books?id=kW3P0FZi9UsC> [Accessed 14<sup>th</sup> August 2013].

Franks, B. (2012) *Taming the Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics*. New Jersey: John Wiley & Sons Inc.

Friese, S. (2011) *The True Qualitative Tool* [ATLAS.ti]. Available from: [http://downloads.atlasti.com/library/friese\\_nl201108.pdf](http://downloads.atlasti.com/library/friese_nl201108.pdf)

Friese, S. (2012) *Qualitative Data Analysis with ATLAS.ti*. London: Sage Publications Inc.

Funtowicz, S. and Ravetz, J. (2003) *International Society for Ecological Economics Internet Encyclopedia of Ecological Economics* [online]. Available from [http://leopold.asu.edu/sustainability/sites/default/files/Norton,%20Post%20Normal%20Science,%20Funtowicz\\_1.pdf](http://leopold.asu.edu/sustainability/sites/default/files/Norton,%20Post%20Normal%20Science,%20Funtowicz_1.pdf) [27<sup>th</sup> July 2012].

Garcia, J. (2005) *Proactive and reactive forensics* [online]. Available from [http://www.jessland.net/docs/Jess\\_Garcia-Proactive\\_and\\_Reactive\\_Forensics.pdf](http://www.jessland.net/docs/Jess_Garcia-Proactive_and_Reactive_Forensics.pdf) [Accessed 4<sup>th</sup> September 2011].

Gershowitz, A. M. and Killinger, L. R. (2011) *The State (Never) Rests: How Excessive Prosecutorial Caseloads Harm Criminal Defendants* [online]. Available from: <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1184&context=nlr> [Accessed 3<sup>rd</sup> October 2013].

Gladney, H. M. (2007) *Preserving Digital Information*. New York: Springer.

Goodman, M. D. (1997) *Why The Police Don't Care About Computer Crime* [online]. Available from: <http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf> [Accessed

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

3<sup>rd</sup> May 2012].

Government Gazette, (2002) Electronic Communications and Transactions Act, 2002 [online]. Available from <http://www.info.gov.za/view/DownloadFileAction?id=68060> [Accessed 25<sup>th</sup> October 2011].

Grady, J. O. (1998) *System Validation and Verification*. Florida: CRC Press LLC.

Gravetter, J. F. and Forzano, L. B. (2009) *Research Methods for the Behavioural Sciences*. 3rd ed. California: Wadsworth.

Greenstein, S. and Stango, V. (2007) Introduction. In: Greenstein, S. and Stango, V. (eds.), *Standards and Public Policy*. New York: Cambridge University Press.

Grindley, P. (1995) *Standards, Strategy and Policy*. New York: Oxford University.

Hall, R. (2012) *Mixed Methods: In Search of a Paradigm* [online]. Available from [http://www.auamii.com/proceedings\\_Phuket\\_2012/Hall.pdf](http://www.auamii.com/proceedings_Phuket_2012/Hall.pdf) [Accessed 30<sup>th</sup> May 2014].

Henry, G. T., Julnes G. and Mark M. M. (1998) *Realist evaluation: An emerging theory in support of practice*. New Directions for Evaluation, No. 78, San Francisco, CA: Jossey-Bass Publishers.

Hoolachan, S. A. and Glisson, W. B. (2010) *Organizational handling of digital evidence* [online]. Available from <https://cas.unisa.ac.za/cas/login?service=https://oasis.unisa.ac.za/wamvalidate%3Furl%3Dhttp%3A%2F%2F0-proquest.umi.com.oasis.unisa.ac.za%3A80%2Fpqdweb%3Findex%3D0%26did%3D2287434051%26SrchMode%3D1%26sid%3D2%26Fmt%3D3%26VInst%3DPROD%26VType%3DPD%26RQT%3D309%26VName%3DPQD%26TS%3D1336062547%26clientId%3D27625> [Accessed 11<sup>th</sup> May 2013].

Hoppenbrouwers, S. J. B. A., Proper, H. A. and van der Weide, Th. P. (2005) *A Fundamental View on the Process of Conceptual Modelling* [online]. Available from <https://pms.cs.ru.nl/iris-diglib/src/getContent.php?id=2004-Hoppenbrouwers-ActOfModelling> [Accessed 7<sup>th</sup> December 2016].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- Hunton, P. (2010) *Cyber Crime and Security: A New Model of Law Enforcement Investigation* [online]. Available from <http://policing.oxfordjournals.org/content/4/4/385.short> [Accessed 12<sup>th</sup> June 2014].
- Interpol, (2013) *Fighting cybercrime worldwide requires law enforcement and private sector to work more closely together, says INTERPOL Chief* [online]. Available from <http://www.interpol.int/News-and-media/News-media-releases/2013/PR043> [14<sup>th</sup> March 2013].
- ITWeb, (2013) *Prosecuting cybercrime a growing problem* [online]. Available from: [http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=63580](http://www.itweb.co.za/index.php?option=com_content&view=article&id=63580) [6<sup>th</sup> August 2013].
- Jaatun, M. G., Albrechtsen, E., Line, M. B., Tondel, I. A. and Longva, O. H. (2009) *A framework for incident response management in the petroleum industry* [online]. Available from <http://www.sciencedirect.com/science/article/pii/S1874548209000043> [Accessed 9<sup>th</sup> June 2014].
- Jones, M. (2000) *Mission impossible? Pluralism and multiparadigm is research* [online]. Available from <https://www.tib.eu/en/search/id/BLCP%3ACN033599493/MISSION-IMPOSSIBLE-PLURALISM-AND-MULTIPARADIGM/> [Accessed 21<sup>st</sup> June 2013].
- Jordaan, J., Barske, D. and Stander, A. and (2010) *A Digital Forensic Readiness Framework for South African SME's* [online]. Available from [http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/30\\_Paper.pdf](http://icsa.cs.up.ac.za/issa/2010/Proceedings/Full/30_Paper.pdf) [Accessed 12<sup>th</sup> October 2016].
- Juta Law. (2016) *FRIEDSHELF 1509 (PTY) LTD t/a RTT GROUP AND OTHERS v KALIANJI 2015 (4) SA 163 (GJ)* [Online]. Available from <https://juta.co.za/profile/login/> [Accessed 2<sup>nd</sup> September 2016].
- Kabanda, S. K., Brown, I., Nyamakura, V. and Keshav, J. (2010) *South African banks and their online privacy policy statements: A content analysis, SA Journal of Information Management* [online]. Available from <http://www.sajim.co.za/index.php/SAJIM/rt/printerFriendly/418/0> [Accessed 7<sup>th</sup> April 2011].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Kebande, V.R. and Venter, H.S. (2016). *On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges* [online]. Available from <http://www.tandfonline.com/doi/abs/10.1080/00450618.2016.1194473> [Accessed 11<sup>th</sup> October 2016].

Kenneally, E. E. and Brown, C. L. T. (2005) *Risk sensitive digital evidence collection* [online]. Available from <http://www.sciencedirect.com/science/article/pii/S1742287605000290> [Accessed 12<sup>th</sup> May 2013].

Kerr, O. S. (2005) *Digital Evidence and The new Criminal Procedure* [online]. Available from [http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1708&context=faculty\\_publications](http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1708&context=faculty_publications) [Accessed 19<sup>th</sup> July 2013].

Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., Butler, R. (2009) *Palantir: A Framework for Collaborative Incident Response and Investigation*, published in *Proceedings of the 8th Symposium on Identity and Trust on the Internet* [online]. Available from <http://0dl.acm.org.oasis.unisa.ac.za/citation.cfm?id=1527017.1527023&coll=DL&dl=ACM&CFID=371942316&CFTOKEN=92269657> [Accessed 15<sup>th</sup> May 2011].

Kizza, J. M. (2007) *Ethical and Social Issues in the Information Age*. 3rd ed. London: Springer.

Kohn, M.D., Eloff, M.M and Eloff, J.H.P. (2013) Integrated digital forensic process model. In: *Computers & Security*, 38, pp. 103-115.

Kotze, D. and Olivier, M.S. (2009) *XBRL-Trail: A Model for Introducing Digital Forensic Readiness to XBRL* [online]. Available from [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=39&ved=0ahUKEwj5msSnmOHPAhVJWhoKHcEYA644HhAWCDEwCA&url=https%3A%2F%2Fwww.cscan.org%2Fopenaccess%2F%3Fid%3D69&usg=AFQjCNG\\_FtUkpTaLNmJ93HOW9OQDHE3spg](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=39&ved=0ahUKEwj5msSnmOHPAhVJWhoKHcEYA644HhAWCDEwCA&url=https%3A%2F%2Fwww.cscan.org%2Fopenaccess%2F%3Fid%3D69&usg=AFQjCNG_FtUkpTaLNmJ93HOW9OQDHE3spg) [Accessed 12<sup>th</sup> October 2016].

Krige, R. (2012) *The Admissibility of Electronically Generated Evidence in a Court of Law*



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

[online]. Available from

[https://docs.google.com/viewer?a=v&q=cache:OW6RDkcGtdsJ:www.lexisnexis.co.za/pdf/Cybercon-1-2-The-Admissibility-of-Electronically-Generated-Evidence-in-a-Court-of-Law-Roux-Krige.ppt+advocate+Roux+Krige&hl=en&gl=us&pid=bl&srcid=ADGEESgR1LU\\_DAOYR RNKqb2BwIFJrPfKxbQKSHi\\_OGOYLE34vx-vLWoGfZkhSotNgzzE3eoTITW2JgOtv6Row2mFOjo-g6M4GqxQzVNPOL5G7BE9f\\_PmFzoAAxDXbgcmdCheA2rHRzL&sig=AHIEtbT61ww017THzNtlIiQC3tJ7\\_SLUzw](https://docs.google.com/viewer?a=v&q=cache:OW6RDkcGtdsJ:www.lexisnexis.co.za/pdf/Cybercon-1-2-The-Admissibility-of-Electronically-Generated-Evidence-in-a-Court-of-Law-Roux-Krige.ppt+advocate+Roux+Krige&hl=en&gl=us&pid=bl&srcid=ADGEESgR1LU_DAOYR RNKqb2BwIFJrPfKxbQKSHi_OGOYLE34vx-vLWoGfZkhSotNgzzE3eoTITW2JgOtv6Row2mFOjo-g6M4GqxQzVNPOL5G7BE9f_PmFzoAAxDXbgcmdCheA2rHRzL&sig=AHIEtbT61ww017THzNtlIiQC3tJ7_SLUzw) [Accessed 16<sup>th</sup> July 2013].

Kvale, S. and Brinkmann, S. (2009) *Interviews: Learning the craft of qualitative research interviewing*. 2<sup>nd</sup> ed. California: Sage Publications.

Kyrö, P. 2014. *The Paradigm and Methodological Choices in Scientific Research*. Available from <https://metodix.fi/2014/03/15/kyro-paula-the-paragidm-and-methodological-choices-in-scientific-research/> [Accessed 22 November 2016].

Lamis, T. 2010 *A forensic approach to incident response* [online]. Available from <http://dl.acm.org/citation.cfm?id=1940975&dl=ACM&coll=DL&CFID=80322195&CFTOKEN=98528235> [Accessed 12<sup>th</sup> August 2013].

Levers, M. D. (2013) *Philosophical Paradigms, Grounded Theory, and Perspectives on Emergence* [Online]. Available from <http://sgo.sagepub.com/content/3/4/2158244013517243> [Accessed 22<sup>nd</sup> November 2016].

Lienhard, A. and Kettiger, D. (2011) *Research on the caseload management of courts: methodological questions* [online]. Available from [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj\\_9b-9tN7QAhVMF8AKHQO5AeMQFggZMAA&url=https%3A%2F%2Fwww.utrechtlawreview.org%2Farticles%2F10.18352%2Ffulr.147%2Fgalley%2F146%2Fdownload%2F&usg=AFQjCNGMov4mYGt073HQ\\_vKSGr4wF8PYug&bvm=bv.139782543,d.ZGg](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj_9b-9tN7QAhVMF8AKHQO5AeMQFggZMAA&url=https%3A%2F%2Fwww.utrechtlawreview.org%2Farticles%2F10.18352%2Ffulr.147%2Fgalley%2F146%2Fdownload%2F&usg=AFQjCNGMov4mYGt073HQ_vKSGr4wF8PYug&bvm=bv.139782543,d.ZGg) [Accessed 6<sup>th</sup> December 2016].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Lillard, T. V., Garrison, C. P., Schiller, C. A. and Steele, J. (2010) *Chapter 9 – Incorporating network forensics into incident response plans: Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data* [online].

Available from <http://0->

[www.sciencedirect.com.oasis.unisa.ac.za/science/article/pii/B9781597495370000090](http://www.sciencedirect.com.oasis.unisa.ac.za/science/article/pii/B9781597495370000090)

[Accessed 15<sup>th</sup> May 2011].

Mackenzie, N. and Knipe, S. (2006) *Research dilemmas: Paradigms, methods and methodology, Issues In Educational Research* [online]. Available from

<http://www.iier.org.au/iier16/mackenzie.html> [Accessed 14<sup>th</sup> April 2014].

Mack, L. n.d. *The Philosophical: Underpinnings of Educational Research* [online]. Available from

[http://www.apu.ac.jp/rcaps/uploads/fckeditor/publications/polyglossia/Polyglossia\\_V19\\_Lindsay.pdf](http://www.apu.ac.jp/rcaps/uploads/fckeditor/publications/polyglossia/Polyglossia_V19_Lindsay.pdf) [23<sup>rd</sup> February 2012].

Mathews, P. (2010) *Sample Size Calculations: Practical Methods for Engineers and Scientists*. Ohio: Mathews Malnar and Bailey Inc.

McConnel International, (2000) *Cybercrime and Punishment? Archaic Laws Threaten Global Information* [online]. Available from

<http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf> [Accessed 6<sup>th</sup> January 2011].

McConnel, J. H. (2005) *How to Develop Essential HR Policies and Procedures*. New York: Amacom.

Miles, M. B and Huberman, A. M. (1994) *Qualitative Data Analysis*. London: Sage Publications Inc.

Mingers, J. (2001) *Combining IS Research Methods: Towards a Pluralist Methodology* [online]. Available from

<http://pubsonline.informs.org/doi/abs/10.1287/isre.12.3.240.9709?journalCode=isr> [Accessed 15<sup>th</sup> June 2015].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Mingers, J. (2004) *Realizing information systems: critical realism as an underpinning philosophy for information systems* [online]. Available from <http://www.bus.iastate.edu/amt/Readings/Theory%20paper%20contemporary/Critical%20Realism%20as.pdf> [Accessed 4<sup>th</sup> June 2015].

Mitchell, J. G. (2005) *Nursing, Philosophy and Knowledge: A commitment to Know Oneself and Others, in Professional Nursing: Concepts, Issues, and Challenges*. (Eds.) Daly, J., Speedy, S., Jackson, D., Lambert V, and Lambert C. NY: Springer.

Morgan, D. L. (2007) *Paradigms Lost and Pragmatism Regained: Methodological Implications of Combining Qualitative and Quantitative Methods*. *Journal of Mixed Methods Research* [online]. Available from <http://www.sagepub.com/gray/Website%20material/Journals/mmr.pdf> [Accessed 1<sup>st</sup> January 2007].

National Institute of Justice, (2001) *Electronic Crime Scene Investigation: A Guide for First Responders* [online]. Available from <http://www.ncjrs.gov/txtfiles1/nij/187736.txt> [Accessed 5<sup>th</sup> April 2010].

Nelson, B., Phillips, A. and Steuart, C. (2010) *Guide to Computer Forensics and Investigations*. 3<sup>rd</sup> ed. Boston: Cengage Learning Inc.

Nelson, S. D., Olson, B. A. and Simek, J. W. (2006) *The Electronic Evidence and Discovery Handbook: Forms, Checklists, and Guidelines*. Chicago: ABA Publishing.

Ngobeni, S., Venter, H. and Burke, I. (2012) *The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks* [online]. Available from [http://www.jucs.org/jucs\\_18\\_12/the\\_modelling\\_of\\_a/jucs\\_18\\_12\\_1721\\_1740\\_ngobeni.pdf](http://www.jucs.org/jucs_18_12/the_modelling_of_a/jucs_18_12_1721_1740_ngobeni.pdf) [Accessed 11<sup>th</sup> October 2016].

Noblett, M. G., Pollitt, M. M. and Presley, L. A. (2000) *Recovering and Examining Computer Forensic Evidence: Forensic Science Communications* [online]. Available from <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=186015> [Accessed 2<sup>nd</sup> March 2010].

NSB, (2007) *Enhancing Support of Transformative Research at the National Science*

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

*Foundation* [online]. Available from [http://www.nsf.gov/nsb/documents/2007/tr\\_report.pdf](http://www.nsf.gov/nsb/documents/2007/tr_report.pdf) [Accessed 23<sup>rd</sup> May 2014].

Obuh, A. O. and Babatope, I. S. (2011) *Cybercrime regulation the Nigerian situation, in Frameworks for ICT Policy: Government, Social and Legal Issues*. Ed. NY: Adomi, E.E. Hershey.

Page, S. B. (2002) *Establishing a System of Policies and Procedures*. Ohio: Process Improvement Publishing.

Palmer, G. (2001) DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research. In: *Digital Forensics Workshop (DFRWS)*. New York: Utica.

Patel, S. (2015) The research paradigm – methodology, epistemology and ontology – explained in simple language [online]. Available from <http://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language> [Accessed 20<sup>th</sup> November 2016].

Pawar, M. (2004) *Data Collecting Methods and Experiences: A guide for social researchers*. New Delhi: New Dawn Press Group.

Pawson, R. and Tilly, N. (1997) *Realistic Evaluation*. London: Sage Publications.

Patton, M. Q. (2002) *Qualitative Research and Evaluation Methods*. California: Sage Publications.

Peltier, T. R. (2005) *Information Security Policies and Procedures: A practitioner's Reference*. 2<sup>nd</sup> ed. Florida: CRC Press LLC.

Prince, A. (2011) *Human Resource Management*. 4<sup>th</sup> ed. Hampshire: Cengage Learning EMEA.

Ramalibana, K. M. (2005) *An investigation into the effectiveness of the staff development policies and programmes of the Unisa Library* [online]. Available from <http://uir.unisa.ac.za/bitstream/handle/10500/2355/?sequence=1> [Accessed 18<sup>th</sup> April 2010].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Randhawa, G. (2007) *Human Resource Management*. New Delhi: Atlantic Publishers and Distributors (P) Ltd.

Reith, M., Carr, C and Gunsch, G. (2002) *An Examination of Digital Forensic Models: International Journal of Digital Evidence* [online]. Available from [http://jjcweb.jjay.cuny.edu/jwkim/class/fcm708/02\\_fall\\_art2.pdf](http://jjcweb.jjay.cuny.edu/jwkim/class/fcm708/02_fall_art2.pdf) [Accessed 3<sup>rd</sup> March 2010].

Reyes, A., Britton, R., O'Shea, K., Steel, J. (2011) *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*. Waltham: Syngress Publishing.

Reyes, A. and Wiles, J. (2007) *The Best Damn Cybercrime and Digital Forensics Book Period*. Burlington: Syngress Publishing Inc.

Rice, P. R. (2005) *Electronic Evidence: Law and Practice*. Chicago: ABA Publishing.

Rogers, M. K. and Seigfried, K. (2004) *The future of computer forensics: a needs analysis survey* [online]. Available from [https://cas.unisa.ac.za/cas/login?service=https://oasis.unisa.ac.za/wamvalidate%3Furl%3Dhttp%3A%2F%2F0-www.sciencedirect.com.oasis.unisa.ac.za%3A80%2Fscience%2Farticle%2Fpii%2FS0167404804000100%3F\\_alid%3D1771163248%26\\_rdoc%3D79%26\\_fmt%3Dhigh%26\\_origin%3Dsearch%26\\_docanchor%3D%26\\_ct%3D6028%26\\_zone%3Drslt\\_list\\_item%26md5%3De5510f538f5e47e117f4fcdeed54da42](https://cas.unisa.ac.za/cas/login?service=https://oasis.unisa.ac.za/wamvalidate%3Furl%3Dhttp%3A%2F%2F0-www.sciencedirect.com.oasis.unisa.ac.za%3A80%2Fscience%2Farticle%2Fpii%2FS0167404804000100%3F_alid%3D1771163248%26_rdoc%3D79%26_fmt%3Dhigh%26_origin%3Dsearch%26_docanchor%3D%26_ct%3D6028%26_zone%3Drslt_list_item%26md5%3De5510f538f5e47e117f4fcdeed54da42) [Accessed 8<sup>th</sup> June 2014].

Rowlingson, R. (2004) *A ten step process for forensic readiness* [online]. Available from <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf> [Accessed 3<sup>rd</sup> May 2010].

Runardotter, M., Quisbert, H., Nilsson J., Hägerfors, A. and Miriamdotter, A. (2005) *The Information Life Cycle – Issues in Long-term Digital Preservation* [online]. Available from [http://www.ltu.se/cms\\_fs/1.82663!/file/TheInformationLifeCycle.pdf](http://www.ltu.se/cms_fs/1.82663!/file/TheInformationLifeCycle.pdf) [Accessed 10<sup>th</sup> August 2013].

SAFLII, (2008) *S v De Vries and Others (67/2005) [2008] ZAWCHC 36 (10 June 2008)*

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

[online]. Available from <http://www.saflii.org/cgi-bin/disp.pl?file=za/cases/ZAWCHC/2008/36.html&query=S%20v%20DE%20VRIES>

[Accessed 23<sup>rd</sup> September 2013].

SAFLII, (2014a). *Bytes Technology Group and Others v Michael (4586/10, 23511/11) [2014] ZAGPPHC 926 (25 November 2014)* [online]. Available from

<http://www.saflii.org/za/cases/ZAGPPHC/2014/926.html> [Accessed 19<sup>th</sup> September 2014].

SAFLII, (2014b). *Ditlhakanyane and Others v S (SS43/2012) [2014] ZAGPJHC 210; 2015 (1) SACR 437 (GJ) (4 August 2014)* [online]. Available from

<http://www.saflii.org/za/cases/ZAGPJHC/2014/210.html> [Accessed 19<sup>th</sup> September 2014].

SAFLII, (2016) *SAFLII Home* [online]. Available from <http://www.saflii.org> [Accessed 25<sup>th</sup> September 2016].

Salmons, J. (2010) *Online Interviews in Real Time*. California: Sage Publications

Sammons, J. (2012) *The Basics of Digital Forensics: the Primer for Getting Started in Digital Forensics*. Waltham: Elsevier Inc.

Schlichting, C. and Mason, J. (2004) *Certification training and the academy* [online].

Available from <http://dl.acm.org/citation.cfm?id=1040253> [Accessed 29<sup>th</sup> August 2015].

Scott, T. A. (2005) *Sample Size Planning, Calculation, and Justification* [online]. Available from

<http://biostat.mc.vanderbilt.edu/wiki/pub/Main/TheresaScott/SampleSize.TAScott.handout.pdf> [Accessed 18<sup>th</sup> December 2017].

Sims, R. R. (2007) *Effective Human Resource Management: Yesterday, Today and Tomorrow*. In: Sims, R. R. (ed.) *Human Resource Management: Contemporary Issues, Challenges, and Opportunities*. Charlotte: Information Age Publishing.

Shalhoub, Z. K. and Qasimi, S. L. A. (2010) *Cyber Law and Cyber Security in Developing and Emerging Economies*. Cheltenham: Edward Elgar Publishing Ltd.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Shavers, B. (2013) *Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. Waltham: Elsevier Inc.

Shinder, L. and Cross, M. (2008) *Chapter 12 - Understanding cybercrime prevention, Scene of the Cybercrime* [online]. Available from <http://www.sciencedirect.com/science/article/pii/B9781597492768000121> [Accessed 15<sup>th</sup> May 2011].

Sobh, T. and Elleithy, K. (2010) *Innovations in Computing Sciences and Software Engineering*. New York: Springer.

South Africa, (2013) *SA Factsheet: South Africa Fast Facts* [online]. Available from <http://www.southafrica.net/country/us/en/content/page/sa-factsheet-enus> [Accessed 21<sup>st</sup> October 2013].

Spivak, S. M. and Brenner, F. C. (2001) *Standardization Essentials: Principles and Practice*. New York: Marcel Dekker Inc.

Stambaugh, H., Beaupre, D., Icove, D., Cassaday, W. and Williams, W. (2001) *State and local law enforcement needs to combat electronic crime* [online]. Available from <https://www.ncjrs.gov/pdffiles1/nij/183451.pdf> [Accessed 9<sup>th</sup> July 2011].

Sutherland, I., Evans, J., Tryfonas, T. and Blyth, A. (2008) *Acquiring volatile operating system data tools and techniques* [online]. Available from <http://dl.acm.org/citation.cfm?id=1368516> [Accessed 28<sup>th</sup> September 2015].

SWGDE (2006) *Scientific Working Group on Digital Evidence* [online]. Available from <https://www.swgde.org/documents/Archived%20Documents/SWGDE%20Data%20Integrity%20Within%20Computer%20Forensics%20V1-0> [Accessed 5<sup>th</sup> December 2016].

Taylor, C., Endicott-Popovsky, B. and Frincke, D.A. (2007) *Specifying digital forensics: A forensics policy approach, Digital Investigation* [online]. Available from <http://dl.acm.org/citation.cfm?id=2296179> [Accessed 23<sup>rd</sup> August 2015].

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Teddlie, C. and Tashakkori, A. (2009) *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. California: Sage Publications.

Thacker, B. H., Doebling, S. W., Hemez, F. C., Anderson, M. C., Pepin, J. E. and Rodriguez, E. A. (2004) *Concepts of Model Verification and Validation* [online]. Available from [http://www.ltas-vis.ulg.ac.be/cmsms/uploads/File/LosAlamos\\_VerificationValidation.pdf](http://www.ltas-vis.ulg.ac.be/cmsms/uploads/File/LosAlamos_VerificationValidation.pdf) [Accessed 10<sup>th</sup> September 2013].

The US Department of Justice, (2009) *Justice Department Hosts International Intellectual Property Program on Advanced Computer and Digital Forensics* [online]. Available from <http://blogs.justice.gov/main/archives/476> [Accessed 2<sup>nd</sup> October 2013].

Unhelkar, B. (2005) *Verification and validation for Quality of UML 2.0 Models*. New Jersey: John Wiley & Sons Inc.

UNISA, (2007) *Policy on Research Ethics* [online]. Available from [http://cm.unisa.ac.za/contents/departments/res\\_policies/docs/ResearchEthicsPolicy\\_apprvCouncil\\_21Sept07.pdf](http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCouncil_21Sept07.pdf) [Accessed 13<sup>th</sup> April 2010].

UNISA, (2010a) *Library* [online]. Available from <http://www.unisa.ac.za/Default.asp?Cmd=ViewContent&ContentID=17> [Accessed 16<sup>th</sup> April 2010].

UNISA, (2010b) *Library: subject databases: a to z - a (off-campus)* [online]. Available from <http://library.unisa.ac.za/infoweb/sbj-db-list.html> [Accessed 16<sup>th</sup> April 2010].

United Nations Radio, (2013) *UN chief urges support for "a robust" international criminal justice system* [online]. Available from <http://www.unmultimedia.org/radio/english/2013/04/un-chief-urges-support-for-a-robust-international-criminal-justice-system/> [4<sup>th</sup> October 2013].

van Baar, R.B., van Beek, H.M.A and van Eijk, E.J. (2014) Digital Forensics as a Service: A Game Changer. In: *Digital Investigation*, 11, pp. 54–62.



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Vacca, J. R. (2005) *Computer Forensics: Computer Crime Scene Investigation*. 2<sup>nd</sup> ed. Massachusetts: Charles River Media Inc.

Venter, J. P. (2006) *Process Flows for Cyber Forensics Training and Operations* [online]. Available from [http://researchspace.csir.co.za/dspace/bitstream/10204/1073/1/Venter\\_2006.pdf](http://researchspace.csir.co.za/dspace/bitstream/10204/1073/1/Venter_2006.pdf) [Accessed 15<sup>th</sup> July 2013].

Verdonck, M. (2014) *Providing guidance for conceptual modelling using core ontologies* [online]. Available from <http://2014.erconference.org/wp-content/uploads/2014/10/Providing-guidance-for-conceptual.pdf> [Accessed 7<sup>th</sup> December 2016].

Vogt, W. P., Vogt W. R., Gardner, D. C. and Haeffele, L. M. (2014) *Selecting the Right Analyses for your data: Quantitative, Qualitative, and Mixed Methods*. New York: The Guilford Press.

Walsh, W., Wolak, J. and Finkelhor, D. (2013) *Prosecution Dilemmas and Challenges for Child Pornography Crimes: The Third National Juvenile Online Victimization Study (NJOV-3)* [online]. Available from [http://www.unh.edu/ccrc/pdf/CV266\\_Walsh\\_Prosecution%20Dilemmas%20for%20CP%20Crimes\\_FINAL\\_1-22-13.pdf](http://www.unh.edu/ccrc/pdf/CV266_Walsh_Prosecution%20Dilemmas%20for%20CP%20Crimes_FINAL_1-22-13.pdf) [Accessed 20<sup>th</sup> May 2013].

Webb, V. (2002) *Language in South Africa: The Role of Language in National Transformation, Reconstruction and Development*. Amsterdam: John Benjamins Publishing Company.

Weber, R. (2004) *The Rhetoric of Positivism Versus Interpretivism: A Personal View* [online]. Available from [misq.org/misq/downloads/download/editorial/25/](http://misq.org/misq/downloads/download/editorial/25/) [Accessed 15<sup>th</sup> September 2012].

Whetten, D.A. (1989) 'What Constitutes a Theoretical Contribution?', *Academy of Management Review*, 14, pp. 490–5.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Wiles, J., Alexander, T., Ashlock, S., Ballou, S., Depew, L., Dominguez, G., Ehuan, A., Green, R., Long, J., Reis, K., Schroader, A., Schuler, K. and Thompson, E. (2007) *Digital forensics: An overview, Techno Security's Guide to E-Discovery and Digital Forensics* [online]. Available from <http://www.sciencedirect.com/science/article/pii/B9781597492232500066> [Accessed 21<sup>st</sup> November 2014].

Wilson, J. P. (2005) *Human Resource Development*. In: Wilson, J. P. (ed.), *Human Resource Development: Learning and Training for Individuals and Organizations*. 2<sup>nd</sup> ed. London: Kogan Page Limited.

Yin, R. K. (2011) *Qualitative Research From Start to Finish*. London: The Guilford Press.

Yusoff, Y., Ismail, R. and Hassan, Z. (2011) *Common Phases of Computer Forensics Investigation Models* [online]. Available from <http://airccse.org/journal/jcsit/0611csit02.pdf> [Accessed 12<sup>th</sup> December 2017].

Zachariadis, M., Scott, S. and Barrett, M (2010) *Exploring critical realism as the theoretical foundation of mixed method research: evidence from the economics of IS innovations* [online]. Available from [http://www.jbs.cam.ac.uk/fileadmin/user\\_upload/research/workingpapers/wp1003.pdf](http://www.jbs.cam.ac.uk/fileadmin/user_upload/research/workingpapers/wp1003.pdf) [Accessed 27<sup>th</sup> July 2014].

Appendix 1: Paper presented at ISSA 2012, South Africa

---

# A conceptual model for digital forensic readiness

Antonio Pooe: Student  
University of South Africa  
1 Preller Street, Muckleneuck Ridge, Pretoria, South Africa  
antonio.pooe@gmail.com

Professor L Labuschagne: Executive Director of Research  
University of South Africa  
1 Preller Street, Muckleneuck Ridge, Pretoria, South Africa  
llabus@unisa.ac.za

**Abstract**—The ever-growing threats of fraud and security incidents present many challenges to law enforcement and organisations across the globe. This has given rise to the need for organisations to build effective incident management strategies, which will enhance the company's reactive capability to security incidents.

The aim of this paper is to propose proactive activities an organisation can undertake in order to increase its ability to respond to security incidents and create a digitally forensic ready workplace environment.

The study constitutes exploratory research, with the use of a systematic literature review as a basis to identify activities relating to a digitally forensic ready environment.

While much has been written about how organisations can prepare to respond to security incidents, findings show an absence of a digital forensic readiness model. This paper concludes by presenting such a conceptual model.

This study contributes to the greater body of knowledge on the design and implementation of a digital forensic readiness programme, aimed at maximising the use of digital evidence in an organisation.

**Keywords** - digital forensic readiness; computer forensics; data integrity; digital evidence; incident handling; empirical research

## 1. Introduction

White-collar crime is a term that has had common occurrence in the news. To explain it, consider the following cases. Towards the end of 1999, the South African government signed contracts totalling R30 billion to modernise its defence equipment. The project, "which promised billions of Rands in export and local sales, has not happened" [1]. On another matter, it was reported that Randgold & Exploration was subject to "massive fraud" equal to R1.5bn by its former CEO Brett Kebble, who misappropriated funds, forged documents and was involved in imprudent deal making, according to a forensic investigation [2]. While these types of cases do not form part of a typical law enforcement agent's daily work, they do depict the gradually decaying ethical fibre of modern-day society. Speculations were that these elaborate crimes would end with Enron, and that the business community would use the lessons learned and better manage this great risk [3]. However, this has not been the case. Many other organisations such as WorldCom, Health South, Adelphia and Tyco suffered the same tragedy [4]. In trying to understand and measure the impact of

fraud on organisations, the Association of Certified Fraud Examiners released findings of a study that a typical organisation loses 5% of its annual revenue to fraud [5]. In other studies, South Africa was found to have the second-worst white-collar crime rate in the world [6].

The inherent risk of increased technical sophistication in modern crimes makes these security incidents harder to detect, thereby potentially creating more damage [7]. Additionally, technology now plays a central role in facilitating and enhancing the sophistication of modern security incidents [8]-[9]. Over the past decade, well-understood procedures and methodologies have evolved within computer forensics digital evidence collection [10]-[11]. Kenneally and Brown [10] further note: "Computer forensic autopsies are no longer performed on single machines with small data storage capacities. Rather, the scope for potential evidence has expanded to networks of interconnected computers, each with vast storage capacities containing potential artefacts of legal relevance". Available literature relating to digital forensic readiness (DFR) addresses various technical components of this concept, but none brings all the components into one framework [12]-[15]. The need for a consolidation of research efforts in creating frameworks and models that help to address recent threats was recently identified by Garfinkel [9], who states that "without a clear strategy for enabling research efforts that build upon one another, forensic research will fall behind the market, tools will become increasingly obsolete, and law enforcement, military and other users of computer forensics products will be unable to rely on the results of forensic analysis".

This paper investigates recent challenges that technology presents with regard to the reliance and admissibility of electronic evidence in a court of law. A systematic literature review was used to gather relevant information and this data is critically analysed in order to identify gaps and to improve upon them.

A section dedicated to explaining the scientific research method adopted in this paper is presented next. This is followed by a section on the application of the said research method, in reviewing existing literature relating to digital forensics. Preceding the conclusion is a section that presents the conceptual model for DFR.

## 2. Research Method

A systematic literature review was used. Unlike conventional literature review, a systematic review follows a predefined protocol. It is defined as a way to "identify, evaluate and interpret the available research that is relevant to an issue or discipline, or phenomenon of interest of a specific research

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

domain” [16]. Systematic reviews require the researcher to systematically collect all the search on a given topic, select studies according to pre-determined quality criteria, abstract the same information from each included study, display the results in evidence tables and interpret the results in view of the totality of the evidence [17].

### A. Scoping

The scope of our research was limited to material available on the University of South Africa Online Library [18]. This library is said to be one of the largest libraries in Africa, best endowed with information sources in access of 1,5 million. The library also subscribes to an increasing number of electronic journals, which are available at all times to Unisa students [18]-[19].

A detailed search of relevant databases was conducted. The relevance was determined by using the library’s A-Z list of electronic resources [18]. From this, only seven databases containing the most relevant material were selected and analysed further for articles and other publications. The databases were selected on the basis of being classified under the following categories:

- Multidisciplinary;
- Computing;
- Law;
- Information Science; and
- Engineering.

Furthermore, the databases that were used were the ones containing the majority of the search hit results. The search term used was “digital forensic”. This keyword was used as the basis of the search as it relates directly to the topic under investigation.

Only English written material published in the last nine years (2002-2011) was considered. The reasons for this were that, firstly, Unisa’s online library is available in English and secondly, English is one of South Africa’s most commonly spoken language in business, politics and the media [20]-[21].

As there was no law on digital crimes in South Africa prior to the Electronic Communications and Transactions Act in 2002 [22], only articles written after promulgation of this law were taken into consideration.

The decision for reviewing only articles was based on the logic that articles usually precede books, dissertations and theses. Therefore, by looking at articles, content from the latter is also covered. The next section deals with the methodology for screening articles for inclusion.

### B. Screening of articles for inclusion

Since the application of a systematic literature review was intended not only for publication purposes but also for instrumental utilisation, an additional task to increase the reliability of the screening process was undertaken. Both the authors conducted the screening process on a subset of articles independently of each other and then met together to compare results.

In order to ensure that this process was scientific, the Cohen’s Kappa (K) interrater was used in measuring reliability of this process. Interrater reliability is the degree of agreement between two observers who have independently observed and

recorded behaviours at the same time [23]-[24]. The basic formula for Cohen’s Kappa (K) used is as computed below:

$$\begin{aligned} \text{Cohen's Kappa} &= \frac{PA(0.77) - PC(0.50)}{1 - PC(0.50)} \\ &= 0.54 \end{aligned}$$

Where PA is the observed percentage agreement and PC is the percentage agreement expected [24].

The goal in this study was to produce a PA value above 75% from the total reviewed articles. This was done to ensure that all relevant articles were included for detailed review and to archive a kappa value above 0.50. The said kappa goal is generally considered to be satisfactory [23]-[24].

Both authors met to calculate the interrater reliability by calculating a percentage agreement. This process was repeated until the percentage agreement exceeded 75%. Abstracts of 459 articles were reviewed, resulting in the identification of 130 relevant articles for possible inclusion. The review process was refined further and the result was an agreement on the final 100 articles for inclusion.

The next section provides a literature overview of DFR.

### 3. Digital Forensic Readiness Overview

Rapid changes and advances in technology and related crimes have given rise to the need to review and improve on digital forensic models and processes. Gravetter and Forzano [25] also make the observation that “unlike other forensic sciences, digital forensics subject matter continues to evolve, as do the techniques”.

Given recent advances in technology, Bell and Boddington [26] argue that it would be imprudent and potentially reckless to rely on existing evidence collection processes and procedures. They add “conventional assumptions about the behaviour of storage media are no longer valid”. Unlike traditional storage media, modern storage devices can operate under their own volition in the absence of computer instructions [10], [27]. Such operations can be highly destructive of traditionally recoverable data. This process has the potential to contaminate evidence and can obfuscate and make validation of digital evidence difficult [10].

For purposes of this study, the use of the term “traditional approaches” denotes forensic procedures undertaken from the dawn of the computer forensic practice to 2005 [10]. First, the basic concept of a traditional approach called dead forensics is explained.

#### A. Dead Forensics

To meet the desired goal of preserving original evidence, one of the first steps in traditional evidence collection procedures includes taking the evidence-containing computer system offline and creating a bit-stream image of the entire original evidence disk [10].

The process begins with the preservation of digital evidence by pulling the power cord, in preparation for the physical removal of the storage device for imaging purposes. Security becomes an important consideration to ensure the logical and physical safety of the evidence. At the conclusion of the imaging process, a hashing tool is used to authenticate the forensic image. This is then followed by the analysis and reporting phases.

Recent studies show that the well-understood digital

# DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

forensic procedures and methodologies are evolving [9], [11]. The scope for potential evidence has expanded from standalone computers to networks of interconnected computers, each with vast storage capacities containing potential artefacts of legal relevance, making the dead forensic process increasingly obsolete.

## B. Live Forensics

Also known as fast forensics, this concept is defined by Reyes and Britton [25] as “those investigative processes that are conducted within the first few hours of an investigation, that provide information used during the suspect interview phase”. Due to the need for information to be obtained in a relatively short time frame, fast forensics usually involves an on-site/field analysis of the computer system in question.

Live analysis techniques use software that existed on the system during the time frame being investigated. On the other hand, dead analysis techniques do not use software that existed on the system during that time frame [28].

Avoiding contamination during the recovery process is paramount and depends on effective, error-free data recovery from digital devices. Traditionally, write-blocking hardware combined with bit-stream image copying processes served this purpose.

Some fast forensics techniques utilise Linux or other forensic boot disks to perform on-scene/site searches and data extraction. The boot disks run in memory only and mount the hard drives as read only so as not to corrupt the evidence [25].

Sutherland et al. [29] agree that “there is no way to avoid making changes, since in order to conduct a live examination it is necessary to deploy tools on the live system to capture data, and such tools will make changes to the running system”.

This argument was later supported by Chan et al. [30], who found that current forensic tools are limited by their inability to preserve the hardware and software state of a system during investigation. Existing tools can overwrite evidence present in memory or alter the contents of the disk causing forensic taint, which lowers the integrity of the evidence.

On the other hand, taking a snapshot of the system can result in a phenomenon known as forensic blurriness, where an inconsistent snapshot is captured because the system is running while it is being observed. Forensic blurriness affects the fidelity and quantity of evidence acquired and can cast doubt on the validity of the analysis, making the courts more reluctant to accept such evidence [30].

From the above, the conclusion is made that neither dead nor live forensics provide sufficient assurance of non-manipulation. Therefore, if existing computer forensic procedures ultimately render evidence inadmissible, then the need for a redefinition of the methodology is paramount.

## C. Digital Forensic Technical Challenges

According to Bell and Boddington [26], “these long-established, internationally accepted procedures even cover situations such as the automated recovery of court-submissible evidence which a defendant has previously attempted to delete. Indeed, the peculiarity of 'deleted, but not forgotten' data which so often comes back to haunt defendants in court is in many ways a bizarre artefact of hard drive technology”.

This comes from the reality that traditional hard disks have slow access speeds relative to their capacity for storage (the latter makes complete erasure very inconvenient), and from the

fact that there is no performance penalty is incurred for writing over existing data (which makes complete erasure unnecessary).

This situation is in the process of changing [9]. Newer technologies such as solid-state drives (SSDs) are much faster and more complex. However, these complexities are not limited only to SSDs, but extend to other storage forms, such as raid arrays, storage area network (SAN) and network attached storage (NAS) devices.

Commensurate changes that need to be made by the digital forensic tool manufacturers to accommodate/address the new file systems, operating systems and connectivity demands also contribute to shorter lifespan of forensic tools [31]. The issue of tools and other technical resources becomes even more pertinent as anti-forensic efforts continue to increase. Anti-forensics can be defined as “the movement to exploit weaknesses in the forensic process or tools” [25].

This rising surge of anti-forensic tools and their ease of access on the internet directly impacts on any organisation's ability, or lack thereof, to respond effectively to digital crimes [32].

There is a need to find a balance between the functionality that security applications provide (eg. secure deletion) and the reverse engineering capability required from digital forensic tools. Findings show that security applications have advanced far beyond digital forensic tools, rendering some forensic tools obsolete against (anti-forensic) actions undertaken using security tools.

## D. Digital Forensic Readiness

The previous section provides evidence suggesting that a mature technical environment alone is not the only factor impacting on the organisation's DFR. In this section, we explore the concept of DFR and other factors that have an impact on it.

Rowlingson [13] defined forensic readiness “as the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation”. Garcia [33] later modified this definition to describe forensic readiness as the “art of maximizing the environment's ability to collect credible evidence”.

From the perspective of law enforcement agencies, the forensic process begins when the crime has been committed or when a crime has been discovered and reported. The concept of forensic readiness, according to Hoolachan and Glisson [34], is that an organisation can pre-empt the occurrence of a crime by preparing the environment in advance and in doing this, organisations will benefit not only in instances where prosecution becomes an issue, but also in limiting their own business risks.

### a) Policies & Procedures

The business requirement to gather and use digital evidence has been recognised in a number of studies. Rowlingson [13] notes that enterprise policies can enhance computer and network forensics. While policies are important, they alone will not guarantee an organisation's overall forensic readiness. An implementation plan (incident response) must be developed and tested.

According to Jaatun et al. [35], incident response is the process of responding to and handling security-related incidents involving information and communications technology

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

infrastructure and data. Incident response has traditionally been rather reactive in nature, focusing mainly on technical issues [35]-[36]. An incident can be anything from an attack that crashes all the servers and cuts off all network communications to an intrusion that causes no actual damage but demonstrates the vulnerability of the organisation's systems [36]-[37]. In the introduction of this article, reference to examples of high-profile fraud cases relating to the South African government's arms deal, Brett Kebble's affairs while at Randgold and those of international companies such as Tyco, Adelphia and WorldCom indicate the damage a poorly managed incident can cause.

Taylor et al. [32] add that "although all security incidents should be taken seriously, they may not all have the same severity". An incident response plan should therefore define how incident severities will be determined and what this means in terms of incident handling.

### b) Incident Management

David [38] suggests that before dealing with "the incidents that have been deemed worthy of treatment, there are three important steps that should be taken. First, all events should be logged, and the logging should be in as much detail as possible". This makes allowance for things such as later treatment of the non-priority items, detecting patterns leading up to incidents, and a ready source of information regarding events that are action items.

The second important step is that there should be an escalating set of responses when appropriate. The benefits derived from this step are what can be called 'quick and dirty' initial reactions to certain incidents, and provide follow-up actions if the earlier ones fail to accomplish their goals.

David [38] further suggests that "all events, even those not designated as incidents to be treated in the incident response plans, should be treated with reasonable promptness, although certainly not with the urgency associated with the more serious events".

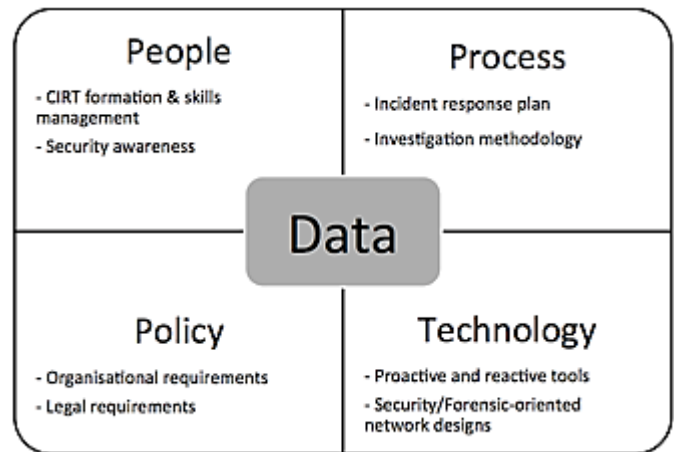
If the above steps are not taken to stop the events of lesser importance, those initiating these events can continue doing them without fear of reprisal, and might even try more severe attacks [37]-[38].

### c) Response Team

In an attempt to be proactive, many organisations form incident response teams—called computer incident response teams (CIRTs). These teams are made up of trained individuals whose goal is to be able to react speedily to occurrences of incidents [39].

Each team member covers a pre-assigned area of responsibility, thus decreasing the amount of damage and increasing the likelihood of apprehending the perpetrator of the incident [35]-[36]. An incident response manager, whose responsibility includes coordinating notifications, escalations and ensuring that the incident response team is properly assembled, usually leads this team [32].

Lamis [39] adds that "communication between team members, internal departments, and external networks is critical to creating a resourceful environment to effectively combat and handle incident responses. An organisation's incident response team may require outside assistance, which costs crucial time and money to select during the incident".



While no evidence of a forensic readiness model could be found, critical components making up such a model can be extrapolated from the literature reviewed. There is a need for a consolidation of research efforts in creating frameworks and models that help to address recent threats and incidents [9]. The next section covers how reviewed literature on research efforts relating to DFR was consolidated in the development of a conceptual model for digital forensic readiness.

### E. Digital Forensic Readiness Conceptual Model

From the literature analysis, the critical components of a DFR model are summarised in Figure 1. At a macro level, core activities relating to DFR fall under four categories, namely People, Process, Policy and Technology. Within each category are sub-activities which can further be classified into proactive and reactive classes.

Figure 1. Digital forensic readiness conceptual model

From the above discussion, forensic readiness as explained by Rowlingson [13] was found to have two main objectives:

- Maximising an environment's ability to collect credible digital evidence; and
- Minimising the cost of forensics during an incident response.

#### a) People

Under the People category are many sub-activities such as the hiring of experienced CIRT members, segregation of duties and security training and awareness campaigns. Establishing a capability for securely gathering legally admissible evidence is a key component of DFR [13].

The objective is to ensure that the human resources of an organisation all contribute towards the prevention and detection of security incidents [14].

Research suggests that building a response team should involve many different organisational departments such as legal and public relations [32], [39]. These additional parties sometimes include external parties who provide support and have skills that may not be present in the organisation.

External parties should also be readily available to provide assistance to internal teams in the event of an incident [36]-[37].

Although the variety of staff involved generally varies depending on the magnitude of the investigation, Hoolachan

# DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

and Glisson [34] argue that “there are a multitude of people who need to understand the correct protocol within a digital investigation”. Failure to organise and equip human resources with the necessary tools and knowledge can ultimately negatively impact the organisation’s forensic readiness.

Developing and documenting processes that affect all parties involved is key in ensuring that the integrity of evidence and the reputation of the organisation remain intact, even after the incident.

## b) Process

The Process category is concerned with activities that ensure the integrity of evidence. This includes ensuring that operational documents such as an incident response plan and a forensic methodology are in place [34]. This is critical as it provides the organisation with an implementation guide to meeting the requirements set by regulatory framework and organisational policies.

Von Solms et al. [14] summarise the four key activities of the digital forensic process:

- 5 Securing the evidence without contaminating it,
- 6 Acquiring the evidence without altering or damaging the original,
- 7 Authenticating that the recovered evidence is the same as the original seized data, and
- 8 Analysing the data without modifying it.

The procedures for evidence acquisition and preservation can be simple, rapid and effective, saving time and money [40]. The complexities of modern network environments, however, demand that organisations define the details well ahead of time. Failing to preserve the integrity of data on a victim or attacking systems in a timely manner will negatively affect the outcome of the investigation.

It is therefore important to have defined processes that guide the organisation in achieving a digitally forensic ready environment. Furthermore, these processes should be governed by certain policies and guiding principles to chart the course of action in the event of an incident.

## c) Policy

Rowlingson [13] notes that enterprise policies can enhance computer and network forensics. In addition, he proposes six categories of policies to facilitate digital forensic investigations. These categories are designed to help enterprises deter computer crime and position themselves to respond to successful attacks by improving their ability to conduct investigations. The six categories of policies that facilitate digital forensic investigations are:

- Retaining information – Policies that relate to the storage of information by an organisation;
- Planning the response – Policies that guide the organisation’s plans to respond to various incidents and situations;
- Training – Policies that address the training of staff members and those affiliated with the organisation;
- Accelerating the investigation – Policies that address operational aspects of investigations;

- Preventing anonymous activities – Policies that address the organisation’s proactive efforts against the risk of fraud; and
- Protecting the evidence – Policies that address the handling and protection of evidence and other vital data.

Grobler and Louwrens [15] argue that digital forensics policies may augment some information security policies, suggesting that interdependencies between policies will exist. As such, these policies must not be developed in silos, but should inform one another.

While policies are important, they alone will not guarantee an organisation’s overall forensic readiness. Technology is the ultimate enabler, ensuring that People have proactive and reactive tools to implement as guided by Policy and defined Processes.

## d) Technology

An organisation needs to ensure that appropriate technology is used not only to enable business operations, but to also prevent and detect computer incidents.

To provide more clarity on the role of technology or system forensic readiness, Tan et al. [40] present the idea of system forensic readiness as one part of overall enterprise forensic readiness. It is critical for organisations to know their sources of potential evidence and to determine what currently happens to the potential evidence data [13].

Evidence preservation is not only affected by technical factors. Tan [12] argues that non-technical factors for consideration also include:

- How logging is done;
- What is logged;
- Intrusion detection systems (IDSs);
- Forensic acquisition; and
- Evidence handling.

According to Doherty and Liebesfeld [31], more private investigators are declining various digital forensic work because the needed and required tools are very expensive and have a short lifespan, due to the increasing and changing variety of digital devices available on the market each year.

The issue of tools and other technical resources becomes even more pertinent as the anti-forensic efforts continue to increase. Anti-forensics, as explained above, can be defined as “the movement to exploit weaknesses in the forensic process or tools” [25]. It can also involve the various acts of hiding data from the forensic exam. Older techniques were as simple as running a simple script to perform a touch command on every file to alter file attributes (date and time stamps), or deleting log and temporary files [41].

It is therefore important to incorporate digital forensic toolsets into the overall organisational technology infrastructure. By including some aspects of DFR into the information security architecture of the organisation, it will be possible to link the source of the attack to the incident and the perpetrator [15]. This integration of digital forensics in the architecture design will help to bridge the gap between advances in security applications and challenges that digital forensic tools face.

# DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

As can be extrapolated from the definition of DFR, efforts to ensure availability and integrity of data are central to maximising the organisation's ability to collect credible evidence to facilitate an investigation [33]-[34]. Studies have also shown that DFR activities relating to data benefit organisations not only in instances where prosecution becomes an issue, but also in limiting an organisation's own business risks [13], [34].

## 4. Value Proposition

As discussed, the increasing sophistication of incidents can cause great harm to an organisation. While numerous organisations have policies, human resources and technical tools, many of these efforts are modelled in a way that supports business functions and not necessarily DFR.

The proposed conceptual DFR model provides a platform for proactive activities to be consolidated and concentrated to ensure collaboration within the organisation in building capacity to prevent, detect and manage incidents.

Additionally, the model can be used to provide a dashboard of all related organisational activities, classified under each of the four components of People, Process, Policy and Technology. Once complete, this classification can be used to measure the maturity of how ready the organisation is to deal with security incidents. This will further aid in reducing duplication of activities geared towards achieving DFR.

## 5. Conclusion

The aim of this paper was to propose proactive activities an organisation can undertake in order to increase its ability to respond to security incidents and create a digitally forensic ready workplace environment. This was done by investigating recent challenges that technology presents with regard to the reliance and admissibility of electronic evidence in a court of law. A systematic literature review was used to gather relevant information and this data was critically analysed in order to identify gaps and to fill them.

Findings show that available literature relating to DFR addresses various technical components of this concept, but none brings all the components into one framework. The need for a consolidation of research efforts in creating frameworks and models that help to address recent threats was also discussed and the outcome is a proposed conceptual DFR model, which can be used as a tool to consolidate and integrate segregated business activities which form part of DFR. The model also identifies four critical components that are necessary to achieve DFR. In the absence of such a model, an organisation will not be able to maximise the environment's ability to collect credible evidence.

Literature reviewed shows that fraud and security incidents affect organisations across the public and private sector. This research adds value by highlighting the impact of technological advances on traditional digital forensic processes. Included is the emphasis on the sophistication of recent security incidents and the importance of a DFR model to aid organisations in aligning efforts that ensure that credible evidence can be retained during normal business operations.

A limitation of this research is that it presents only a conceptual model, which is generic in nature. Further research opportunities are in building on the proposed conceptual model by identifying the different stakeholders in an investigation process, and personalising the model to their varying environments. Additionally, sub-activities within each of the

identified components of the model can be investigated in greater detail, to include testing of recent forensic and security tools that can be used to address technological advances discussed earlier in this paper.

## 6. Acknowledgment

A special thanks to the library team at the University of South Africa for their diligence in ensuring that all articles required for this study were purchased and made available on the UNISA online study resources.

## 7. References

- [1] Mail & Guardian. (2008, August). *Mbeki 'paid R30m arms-deal bribe*. [Online]. Viewed 2011 October 7. Available: <http://www.mg.co.za/article/2008-08-03-mbeki-paid-r30m-armsdeal-bribe>
- [2] D. McKay. (2006, March). *Kebble fraud unpacked*. [Online]. Viewed 2011 October 7. Available: <http://www.miningmx.com/news/archive/150120.htm>
- [3] T. Brazley, *Investigating While Collar Crime*, New Jersey: Pearson Education, 2008.
- [4] T. Dimnik. (2010, May). *The "unified perspective" recipe for a successful compliance program*. Viewed 2011 October 7. Available: <http://www.itcba.org/dynamicdata/flash/3-%20May%2020.ppt>
- [5] ACFE. (2010). *Report to the nation on occupational fraud and abuse*. [Online]. Viewed 2011 October 3. Available: <http://www.acfe.com/rtnn/rtnn-2010.pdf>
- [6] PWC. (2009). *The 5th Global Economic Crime Survey*. [Online]. Viewed 2011 October 3. Available: [http://www.pwc.com/en\\_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf](http://www.pwc.com/en_GX/gx/economic-crime-survey/pdf/global-economic-crime-survey-2009.pdf)
- [7] KPMG. (2009). *E-crime survey*. [Online]. Viewed 2011 October 3. Available: [http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009\\_AKJ\\_KPMG\(1\).pdf](http://www.e-crimecongress.org/ecrime2009/documents/e-CrimeSurvey2009_AKJ_KPMG(1).pdf)
- [8] S. Peters. (2009). *14th Annual CSI Computer Crime and Security Survey*. [Online]. Available: <http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf>
- [9] S. L. Garfinkel. (2010, August). Digital forensics research: The next 10 years. *Proceedings of the Tenth Annual DFRWS Conference*. [Online]. 7, pp. S64-S73. Available: <http://www.sciencedirect.com/science/article/pii/S1742287610000368>
- [10] E. E. Kenneally, and C. L. T. Brown. (2005, February). Risk sensitive digital evidence collection. *Digital Investigation*. [Online]. 2, pp. 101-119. Available: <http://www.sciencedirect.com/science/article/pii/S1742287605000290>
- [11] P. Cooper, G. T. Finley and P. Kaskenpalo. (2010, June). Towards standards in digital forensics education. *Proceedings of the 2010 ITiCSE Working Group Reports*. [Online]. 10, pp. 26-30. Available: [http://0-delivery.acm.org.oasis.unisa.ac.za/10.1145/1980000/1971688/p87-cooper.pdf?ip=163.200.81.46&acc=ACTIVE%20SERVICE&CFID=80236719&CFTOKEN=73481127&\\_\\_acm\\_\\_=1336017593\\_fdcbf3197899faba4a384fcf3d289e65](http://0-delivery.acm.org.oasis.unisa.ac.za/10.1145/1980000/1971688/p87-cooper.pdf?ip=163.200.81.46&acc=ACTIVE%20SERVICE&CFID=80236719&CFTOKEN=73481127&__acm__=1336017593_fdcbf3197899faba4a384fcf3d289e65)
- [12] J. Tan. (2001, July). *Forensic readiness*. [Online]. Available: [http://isis.poly.edu/kulesh/forensics/forensic\\_readiness.pdf](http://isis.poly.edu/kulesh/forensics/forensic_readiness.pdf)
- [13] R. Rowlingson. (2004). *A ten step process for forensic readiness*. [Online]. Available: <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf>



# DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

- [14] S. von Solms, C. Louwrens, C. Reekie, and T. Grobler. (2006). A control framework for digital forensics. *IFIP Advances in Information and Communication Technology*. [Online]. 222, pp. 343-355. Available: <http://www.springerlink.com/oasis.unisa.ac.za/content/978-0-387-36890-0/#section=684286&page=12&locus=45>
- [15] C. P. Grobler, and C. P. Louwrens. (2007). New approaches for security, privacy and trust in complex. *IFIP International Federation for Information Processing*. [Online]. 232, pp. 13-24. Available: <http://www.springerlink.com/oasis.unisa.ac.za/content/r82m17v470581t34/?MUD=MP>
- [16] T. Sobh, and K. Elleithy, *Innovations in Computing Sciences and Software Engineering*, New York: Springer, 2010.
- [17] T. A. Lang, *How To Write, Publish, & Present in the Health Sciences: A Guide for Clinicians & Laboratory Researchers*, 2<sup>nd</sup> ed., Philadelphia: American College of Physicians, 2010.
- [18] University of South Africa. (undated). [Online]. Viewed 2011 December 11. Available: <http://www.unisa.ac.za>
- [19] K. M. Ramalibana. (2005, December). *An investigation into the effectiveness of the staff development policies and programmes of the Unisa Library*. [Online]. Available: [http://uir.unisa.ac.za/handle/10500/5/browse?order=ASC &rpp=20&sort\\_by=1&etal=-1&offset=20&type=title](http://uir.unisa.ac.za/handle/10500/5/browse?order=ASC &rpp=20&sort_by=1&etal=-1&offset=20&type=title)
- [20] V. Webb, *Language in South Africa: The Role of Language in National Transformation, Reconstruction and Development*, Amsterdam: John Benjamins, 2002.
- [21] South Africa. (2012, March). *The languages of South Africa*. [Online]. Viewed 2012 April 12. Available: <http://www.southafrica.info/about/people/language.htm>
- [22] S. K. Kabanda, I. Brown, V. Nyamakura, and J. Keshav. (2010). South African banks and their online privacy policy statements: A content analysis. *SA Journal of Information Management*. [Online]. 12 (1). Available: <http://www.sajim.co.za/index.php/SAJIM/rt/printerFriendly/418/0>
- [23] P. Mathews. *Sample Size Calculations: Practical Methods for Engineers and Scientists*, Ohio: Mathews Malnar and Bailey Inc, 2010.
- [24] J. F. Gravetter, and L. B. Forzano, *Research Methods for the Behavioral Sciences*, 3rd ed., California: Wadsworth, 2009.
- [25] A. Reyes, and R. Britton, *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement, and Prosecutors*, Waltham: Syngress Publishing, 2007.
- [26] G. Bell, and R. Boddington. (2010, July). Solid state drives: The beginning of the end for current practice in digital forensic recovery. *The Journal of Digital Forensics, Security and Law*. [Online]. 5 (3), pp. 5-32. Viewed 2011 June 9. Available: <http://www.proquest.com/oasis.unisa.ac.za/>
- [27] F. Chen, D. A. Koufaty, and X. Zhang. (2009). *Understanding intrinsic characteristics and system implications of flash memory based solid state drives*. [Online]. Available: <http://www.cse.ohio-state.edu/hpcs/WWW/HTML/publications/abs09-2.html>
- [28] B. D. Carrier. (2006, February). Risks of live digital forensic analysis. *Communications of the ACM - Next-generation cyber forensics* [Online]. 49 (2), pp. 1-38. Available: <http://dl.acm.org/oasis.unisa.ac.za/citation.cfm?id=1113034.1113069&coll=DL&dl=ACM>
- I. Sutherland, J. Evans, T. Tryfonas, and A. Blyth. (2008, April). Acquiring volatile operating system data tools and techniques. *ACM SIGOPS Operating Systems Review*. [Online]. 42 (3), pp. 65-73. Available: [http://dl.acm.org/oasis.unisa.ac.za/citation.cfm?id=1368506.1368516&coll=DL&dl=ACM&ticket=](http://dl.acm.org/oasis.unisa.ac.za/citation.cfm?id=1368506.1368516&coll=DL&dl=ACM&ticket=ST-263623-X2KUjNq4oUAqGKcSq5E5-cas)
- [29] E. Chan, S. Venkataraman, F. David, A. Chaugule, and R. Campbell. (2010, December). Forenscope: A framework for live forensics. *Proceedings of the 26th Annual Computer Security Applications Conference*. [Online]. 26, pp. 307-316. Available: <http://dl.acm.org/oasis.unisa.ac.za/citation.cfm?id=1920261.1920307&coll=DL&dl=ACM&ticket=ST-263647-PHrEuXlSz0pJNKsP4ULH-cas>
- [30] E. Doherty, and J. Liebesfeld. (2008, May). Proposing a digital forensics grange. *Security*. [Online]. 45 (5), pp. 32-33. Available: <http://proquest-umi-com-oasis-unisa-ac-za/pqdweb?did=1480181371-&sid=1-&Fmt=3-&clientId=27625-&RQT=309-&VName=PQD>
- [31] C. Taylor, B. Endicott-Popovsky, and D. A. Frincke. (2007, September). Specifying digital forensics: A forensics policy approach. *Digital Investigation*. [Online]. 4 (1), pp. 101-104. Available: <http://www.sciencedirect.com/oasis.unisa.ac.za/science/article/pii/S1742287607000461>
- [32] J. Garcia. (2005, September). *Proactive and reactive forensics*. [Online]. Available: <http://jessland.net/Docs.php>
- [33] S. A. Hoolachan, and W. B. Glisson. (2010, May). Organizational handling of digital evidence. *Proceedings of the Conference on Digital Forensics, Security and Law*. [Online]. pp. 33-44. Available: <http://proquest.umi.com/oasis.unisa.ac.za/pqdweb?index=0&did=2287434051&SrchMode=1&sid=2&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1336062547&clientId=27625>
- [34] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tondel, and O. H. Longva. (2009, March). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection*. [Online]. 2 (1-2), pp. 26-37. Available: <http://www.sciencedirect.com/science/article/pii/S1874548209000043>
- [35] L. Shinder, and M. Cross. (2008, June). Chapter 12 – Understanding cybercrime prevention. *Scene of the Cybercrime*, 2<sup>nd</sup> ed., [Online]. pp. 505-554. Available: <http://www.sciencedirect.com/oasis.unisa.ac.za/science/article/pii/B9781597492768000121>
- [36] T. V. Lillard, C. P. Garrison, C. A. Schiller, and J. Steele. (2010, June). Chapter 9 – Incorporating network forensics into incident response plans. *Digital Forensics for Network, Internet, and Cloud Computing – A Forensic Evidence Guide for Moving Targets and Data*. [Online]. pp. 221-274. Available: <http://www.sciencedirect.com/oasis.unisa.ac.za/science/article/pii/B9781597495370000090>
- [37] J. David. (2000, February). Incident response. *Network Security*. [Online]. 1999 (11), pp. 15-18. Available: <http://www.sciencedirect.com/science/article/pii/S1353485800800057>
- [38] T. Lamis. (2010, October). A forensic approach to incident response. *Information Security Curriculum Development Conference*. [Online]. pp. 177-185. Available: <http://dl.acm.org/citation.cfm?id=1940975&dl=ACM&coll=DL&CFID=80322195&CFTOKEN=98528235>
- [39] T. Tan, T. Ruighaver, and A. Ahmad. (2003, November). *Incident handling: Where the need for planning is often not recognised*. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1353485800800057>
- [40] J. Wiles, T. Alexander, S. Ashlock, S. Ballou, L. Depew, G. Dominguez, A. Ehuan, R. Green, J. Long, K. Reis, A. Schroader, K. Schuler, and E. Thompson. (2007). Chapter 2 - Digital forensics: An overview. *Techno Security's Guide to E-Discovery and Digital Forensics*. [Online]. pp. 33-63.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA  
HANDLING**

Available: [http://www.sciencedirect.com/science/  
article/pii/B9781597492232500066](http://www.sciencedirect.com/science/article/pii/B9781597492232500066)

**Appendix 2: Paper presented at IFIP 2014, United States of America**

---

**COGNITIVE APPROACHES FOR HOLISTIC DIGITAL FORENSIC READINESS  
PLANNING**

Antonio Poee and Les Labuschagne

**Abstract**

This paper focuses on the use of cognitive approaches for digital forensic readiness planning. Research has revealed that a well-thought-out and legally contextualized digital forensic readiness strategy can provide organisations with an increased ability to respond to security incidents while maintaining the integrity of the evidence gathered and keeping investigative costs low. This paper contributes to the body of knowledge in digital forensics related to the design and implementation of digital forensic readiness plans aimed at maximizing the use of digital evidence in organisations. The study uses interviews as part of a mixed-methods approach. In particular, it employs a mix of informal conversational and standardized open-ended interview styles conducted with industry experts over a variety of communication media.

**Keywords:** *digital forensic readiness; digital evidence; cognitive approaches*

**1. Introduction**

From the perspective of law enforcement agencies, the forensic process begins when a crime has been committed or when a crime has been discovered and reported [6]. Forensic readiness enables organisations to preempt the occurrence of crimes by gathering evidence in advance and, in doing so, derive benefits in instances where prosecution becomes an issue and also limit their risks [5].

The organisational requirement to gather and use digital evidence has been recognized in a number of studies (see, e.g., [2, 5]). These studies stress the importance of a structure to

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

maintain the integrity of forensic evidence. In particular, Yasinsac and Manzano [7] note that organisational policies play a critical role in providing the needed structure. Yasinsac and Manzano also propose six categories of policies to facilitate digital forensic investigations. The categories are designed to help organisations deter digital crime and position themselves to respond to attacks by improving their ability to conduct investigations. The six categories of policies that facilitate digital forensic investigations are:

- **Retaining Information:** Policies that relate to the storage of information by an organisation.
- **Planning the Response:** Policies that guide an organisation's plans for responding to incidents and situations.
- **Training:** Policies that address the training of staff members and others affiliated with an organisation.
- **Accelerating the Investigation:** Policies that address the operational aspects of investigations.
- **Preventing Anonymous Activities:** Policies that address an organisation's proactive efforts against fraud.
- **Protecting the Evidence:** Policies that address the handling and protection of evidence and other vital data.

From the above discussion, the concept of digital forensic readiness has two main objectives: (i) maximizing the ability to collect credible digital evidence (Categories 1, 2, 5 and 6 above); and (ii) minimizing the cost of digital forensics during incident response (Categories 3 and 4). While this reinforces the importance of cohesive policies in organisations, the problem with the categorisation is that it suggests that organisations must have all six policies in place, which may result in possible duplication and/or conflicting policy statements. Furthermore, it may lead to confusion in identifying the authority/governing policy for facilitating digital investigations. While the policies are important, they alone do not guarantee

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

a holistic digital forensic readiness plan.

Because of the potential policy conflicts, this study used mixed methods interviews [4] as a means to develop a holistic digital forensic readiness plan. The interviews were employed as an exploratory research tool to gather information from subject matter experts and to capture real-world experiences with the goal of identifying key components for consideration.

### **2. Research Design**

Mixed method research is a design with philosophical assumptions and various methods of inquiry [4]. The philosophical assumptions guide the direction of the collection and analysis of data while the combination of qualitative and quantitative methods of inquiry in a single or series of studies offers a better understanding of research problems than each approach on its own [12].

The intent of the two-phase exploratory design is that the results of the first method (qualitative) can help develop or inform the second method (quantitative) [4]. This is based on the premise that an exploration may be needed for one or more reasons, which takes into account the possibility that measures or instruments are not available, variables are unknown and no guiding framework or theory exists.

This design is used because it enables the exploration of a phenomenon in detail and the development and testing of the resulting conceptual model [4, 12]. The use of the design in this study helps validate qualitative data with quantitative results.

Interviews were used in this study as the data collection method. In mixed methods research, open-ended qualitative interviews (INTQUAL) are featured more frequently than closed-ended quantitative interviews (INT-QUAN). Qualitative interviews are usually non-directive and general ("tell me about your school"). On the other hand, quantitative interviews are structured and closed-ended ("which of the following describes the food in your school cafeteria - very good, good, bad, very bad") [12].

## **2.1 Types of Interviews**

Patton [8] defined four types of open-ended interviews, ranging from the least structured (informal conversational interviews) to more structured (general interview-guided approaches) to the most structured (standardized open-ended interviews). He also described closed fixed-response interviews but does not advocate their use. The four types of open-ended interviews are:

- **Type 1: Informal Conversational Interview:** Questions emerge from the immediate context and are asked in the natural course of the interview. The question topics and wording are not predetermined.
- **Type 2: General Interview Guide Approaches:** Topics and issues are specified in advance in outline form. The interviewer decides the sequence and working of questions in the course of the interview.
- **Type 3: Standardized Open-Ended Interviews:** The exact wording and sequence of questions are determined in advance. All interviewees are asked the same basic questions in the same order. Questions are worded in a completely open-ended format.
- **Type 4: Closed Fixed-Response Interviews:** Questions and response categories are determined in advance. The responses are fixed. The respondent chooses from among the fixed responses.

For purposes of this study, a mixture of Type 1 and Type 3 open-ended interviews was used. Teddie and Tashakkori [12] state that researchers who select the INT-QUAL strategy may use any of the open-ended interview approaches and potentially combine the interview types. They suggest the following sequence of interview techniques:

Figure 1. Start with the unstructured informal conversational interview approach to build rapport and elicit spontaneous responses.

## **DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING**

Figure 2. Move to the interview guide approach that provides a more comprehensive outline of topics, but yet maintains a conversational tone.

Figure 3. Finish with the highly structured, standardized open-ended interview approach, which greatly increases response comparability.

Our study began with an unstructured informal conversational interview approach, followed by a highly structured, standardized open-ended interview approach. The questions were formulated based on a literature survey conducted in 2011 [9].

### **2.2 The Interviews**

This section discusses the criteria used to select the interviewees, the communication channels used to conduct the interviews and the ethical considerations related to the interview process.

The interviewees were selected based on three criteria:

- Individuals from the private sector and law enforcement were selected in order to emphasize the multidisciplinary aspects of the domain and to capture a broad range of views from subject matter experts involved in different aspects of the digital forensic process.
- Individuals with experience in digital law and/or digital forensics were selected to ensure that the input gathered was not biased and addressed the technical and legal dimensions of digital forensics.
- Individuals who had been practicing digital forensics in South Africa for a period of no less than three years were selected. Since the context of the study was South Africa, it was important to identify subject matter experts with experience in the geographical context.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

*Table 1 – Interviewee profiles*

Interviewee	Experience > 3 Years	Law Enforcement	Private Sector Experience	Management Position
INT1	Yes	Yes	No	Yes
INT2	Yes	Yes	Yes	Yes
INT3	Yes	No	Yes	Yes
INT4	Yes	Yes	Yes	Yes
INT5	Yes	No	Yes	Yes
INT6	Yes	Yes	No	Yes
INT7	Yes	Yes	Yes	Yes

These criteria ensured that the interviewees would provide a mixture of opinions based on their experiences in their different working environments. Studies have shown that while open-ended interviews are typically conducted in a face-to-face manner, they may also be conducted over the telephone and via the Internet [11, 12].

A total of seven interviews were conducted using three channels: four interviews were face-to-face, one was conducted over the phone and two over the Internet. Due to the volume of data collected, the ATLAS.ti tool [1] was used to process and analyse the data collected during the interviews.

### **3. Interview Results**

This section describes the results of the seven interviews. All the interviewees met the selection criteria. Table 1 summarizes the interviewee profiles.

We now provide a summary of some of the questions, the responses received and the interviewees that were in agreement. Based on the responses, cognitive approaches to digital forensic readiness planning were used to develop a conceptual model.

- i. Question 1: Should South African organisations be concerned about digital crimes?*

Responses to this question show the following opinions:

- j. Digital crimes were on the increase (All).*
- k. The intangible nature of data in electronic format causes people to lower their*



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

defences (INT1, INT4 and INT7).

- l. Modern criminals are technologically literate and have access to good legal representation (INT1, INT2 and INT3).
- m. Immaturity of the digital forensic profession allows criminals to go free (INT5).
- n. Following correct investigative processes to preserve evidence is important (INT6).

ii. *Question 2: Which three types of digital crimes do you find to be the most prevalent?*

The following crimes were found to be prevalent:

- o. Financial crimes (All).
- p. Child pornography (INT4, INT5, INT6, INT7).
- q. 419 scams (INT4, INT6).
- r. Malware-related crimes (INT1, INT2).
- s. Intellectual property theft (INT1, INT5).
- t. Hacking and illegal access (INT3, INT2).
- u. Internet misuse (INT5).

iii. *Question 3: Which sector do you find to be the most targeted?*

The following sectors were found to be targeted:

- v. Banks/financial Sector (All).
- w. Large corporates (INT2, INT4 and INT7).
- x. Individuals (INT2 and INT3).
- y. Mining (INT4).
- z. Businesses (INT5).

iv. *Question 4: Have you noted any challenges regarding the prosecution of digital crimes?*

The following challenges were noted:

- aa. Knowledge of digital forensic principles lacking among the stakeholders (All).
- bb. Lack of understanding of legal requirements (INT1; INT3; INT4, INT5, INT6).

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

cc. Lack of resources [INT2, INT7].

- v. *Question 5: Do you or your organisation have a digital forensic model that has been adopted?*

All the respondents indicated that they use their own entity-specific model, which may differ from those used by other organisations.

- vi. *Question 6: Does electronic evidence provide sufficient assurance of non-manipulation?*

Provided that the correct processes were followed, all the respondents were of the opinion that electronic evidence can be relied upon.

- vii. *Question 7: Is there a standard process for electronic evidence gathering?*

All the respondents indicated that, while processes adopted in their individual organisations were similar, no process standards specific to South Africa exist.

- viii. *Question 8: Does the law adequately position the acceptable use of/or extent to which electronic evidence can be used in a civil or criminal proceedings?*

All respondents referred to the Electronic Communications and Transactions (ECT) Act of 2002 as legislation that makes it possible to present electronic evidence in a South African court of law. However, the following contradictions were noted:

dd. Existing laws support the ECT Act (INT4, INT5 and INT7).

ee. Discrepancies exist between ECT Act and existing laws (INT2).

- ix. *Question 9: Does the law cater to the complexities of modern IT devices?*

All the respondents indicated that the law lagged behind technology. While the ECT Act was found to be strong legislation, the respondents indicated that it needed periodic review.

- x. *Question 10: What are the factors that contribute to electronic evidence being rendered inadmissible?*

All the respondents pointed to digital forensic processes and procedures as a good

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

foundation for ensuring the admissibility of evidence.

- xi. Question 11: Have you noted any challenges that prevent digital crime investigators from correctly applying the digital forensic model or framework?*

All respondents indicated that a single point of reference was needed. Other points noted were:

- ff. South Africa needs a specific model (INT5 and INT7).
- gg. The model must enable and support legal processes (INT7).
- hh. The model must be flexible (INT5).

- xii. Question 12: Do you think digital forensic investigators are sufficiently trained to do their work?*

All the respondents identified a need for more training for local digital forensic investigators.

- xiii. Question 13: Have you noted any challenges that prevent prosecutors from successfully prosecuting digital crimes?*

Responses identified the following challenges:

- ii. A lack of interest in digital crimes (INT1, INT3, INT4, INT5, INT 6, INT 7).
- jj. High caseloads (INT1, INT2, INT4, INT5 and INT7).
- kk. Lack of digital forensic training and/or awareness (INT2, INT5 and INT7).
- ll. Lack of cooperation (INT5).

- xiv. Question 14: Do you think state prosecutors are sufficiently trained to do their work?*

All respondents opined that a training need exists for state prosecutors.

- xv. Question 15: What do you think should be done to increase the prosecution rate of digital crimes in South Africa?*

The responses included:

- mm. Special digital forensic courts (INT1, INT3, INT4, INT5 and INT7).

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

- nn. Education, training and awareness (INT1, INT2, INT6 and INT7).
- oo. More research focused on digital forensics (INT1 and INT6).
- pp. Compulsory reporting requirements (INT1 and INT5).
- qq. A new law of evidence for electronic crimes (INT2).
- rr. Define processes and a model (INT4).

### 4. Data Analysis and Interpretation

This section discusses the application of the data analysis method and presents the results of the analysis.

The data analysis was conducted by transcribing each interview and reading each transcript repeatedly to identify the codes for each question answered by the interviewees. Techniques from immersion/crystallisation and constant comparison (grounded theory) were applied to assist with the development of the initial and final codes [3]. The iterative reading process made it possible for focus/immersion to be applied to each question and for the emergence/crystallisation of themes to take place. Differences in findings (codes and themes) were also resolved using the iterative process. The above process resulted in three environments: corporate, industry and legislative.

#### 4.1 Corporate Environment

Key findings from the correlation of results from each interview revealed the following:

- **Organisational Culture:** A large proportion of organisations were found to have a habit/culture of ignoring/overlooking small crimes. Additionally, organisations were found to invest the least amount of resources to address the risk of digital crimes. Finally, a lack of awareness about digital crime prevention and detection was found to exist.

These findings suggest that, by creating a culture of no tolerance to crime and

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

taking action on reported crimes, an organisation can significantly reduce its risk exposure to digital crimes.

- **Policies:** Interviewees noted that a general lack of governance, policies and procedures relating to fraud risk management existed in many of the organisations with which they had been in contact. These findings support existing literature (as discussed earlier in this study) on the importance of policies as they relate to achieving digital forensic readiness.
- **Communication Channels:** The reporting of digital crimes was found to be low. The causes mentioned included a culture of “sweeping things under the carpet” along with ignorance, and the lack of education and law enforcement effectiveness.

These findings suggest that encouraging and supporting open dialog, coupled with crime reporting mechanisms can positively impact organisational culture.

- **Emerging Risks:** The following areas of risk were identified:
  - The intangible aspect of technology causes people to lower their defences. This is evident in the various types of white-collar crimes committed using technology.
  - Modern IT criminals are technologically literate and have access to financial and other resources, including good legal representation.
  - Criminals are quick to exploit innovations in mobile technology.
  - The digital forensic industry is not sufficiently mature, enabling criminals to take advantage of ambiguities in global legal structures.
  - Digital forensic investigators often do not follow due process, which contributes to the low prosecution rate of digital crimes.

The findings suggest the importance of being cognizant about emerging risks because they affect the nature of controls and mitigation strategies that organisations

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

employ.

- **Crime Trends:** Respondents were of the opinion that digital crimes are on the increase and will affect all current and future users of technology. The high prevalence of crime is attributed to legal gaps. These findings suggest that increased awareness of crime trends can aid organisations in focusing their attention and resources on high risk areas.

### 4.2 Industry Environment

The correlation of results from each interview revealed the following findings:

- **Standards:** The absence of standards for digital forensics was identified as an inhibiting factor to the prosecution of digital crimes. An open culture of information sharing was noted as necessary to promote the maturity of the digital forensic profession. Specific to a digital forensic model, this should not be legislation but, instead, recommended guidelines that enable and support the legal process while being sufficiently flexible to accommodate advances and changes in legislation and technology.

These findings suggest that establishing governance structures is an important step to building quality digital forensic case law and professionalizing the digital forensic industry.

- **Methodology:** While digital forensic investigation methodologies exist, there is a need for a single point of reference. This extends to the need for consistency in country-specific standards, processes and methodology. Awareness of research-based methodologies and their alignment to legislation was also found to be necessary.

These findings suggest that standardisation can encourage consistency, conformity, compliance and increase competitiveness in the digital forensic profession.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

- **Education:** A lack of cohesion between academics and practitioners was found to exist. While interviewees noted that no single qualification is a prerequisite to qualify as a digital forensic practitioner, specialized training and a balance of education and experience were found to be necessary. A digital forensic model was also found to be essential to guide training efforts.

These findings suggest that the ideal qualification requirements for digital forensic practitioners are formal education coupled with advanced training in a field of specialisation.

- **Training:** Training of all stakeholders was noted as essential. In particular, emphasis was placed on legal requirements as superseding technical processes. Some practitioners lack an understanding of the legal requirements and/or incorrectly apply technical knowledge. These findings suggest the need to expose digital forensic investigators to a balanced training curriculum that covers all related disciplines.
- **Development:** There was a lack of continued professional development for individuals in the investigation value chain, including prosecutors, judges and digital forensics practitioners across all sectors. These findings suggest the need for organisations to employ qualified digital forensic investigators and provide continuous education and career development in order to ensure that the investigators are equipped with the skills necessary to handle modern digital crimes.

### 4.3 Legislative Environment

The correlation of results from the interviews yielded the following findings:

- **Legal Culture:** A lack of consideration of digital crimes exists among some judges and prosecutors; this was attributed to high caseloads and limited resources. The creation of special interest groups and special courts could

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

introduce positive changes. These findings suggest the need for a culture of cooperation between organisations, law enforcement and prosecuting authorities.

- **eLaw Development:** Specific to South African legislation on electronic evidence [10], the findings indicate that the key strengths of the law are robust legislation and good baselines. On the other hand, the findings also suggest that the law imposes low penalties, there is limited awareness and understanding of the law, and considerable complexity in its use of technical terminology. Lastly, the South African legislation on electronic evidence was perceived as being adequate to cover technological advances over the next ten to twenty years. These findings suggest the need for continuous review and development of legislation relating to digital crimes in order to close the gap (of relevance) between technology and the law.
- **Awareness:** The findings suggest that the judiciary is presented with challenges that result in a reluctance to prioritize digital evidence. High caseloads and a lack of awareness of digital forensic processes and methodologies exist. Interviewees pointed to a need for a change in culture. Training and awareness were suggested as effective drivers to implement this change. These findings point to the importance of digital forensic awareness initiatives as a means to reduce the reluctance to prioritize digital crimes and increase confidence levels when prosecuting crimes.

### 5. Cognitive Approaches

From the breadth of responses and the associated analysis, it is clear that the development of a digital forensic readiness plan extends beyond the realm of an organisation. The corporate, industry and legislative environments each have properties that must be considered when developing a digital forensic readiness plan. These properties are presented in Figure 1.



## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

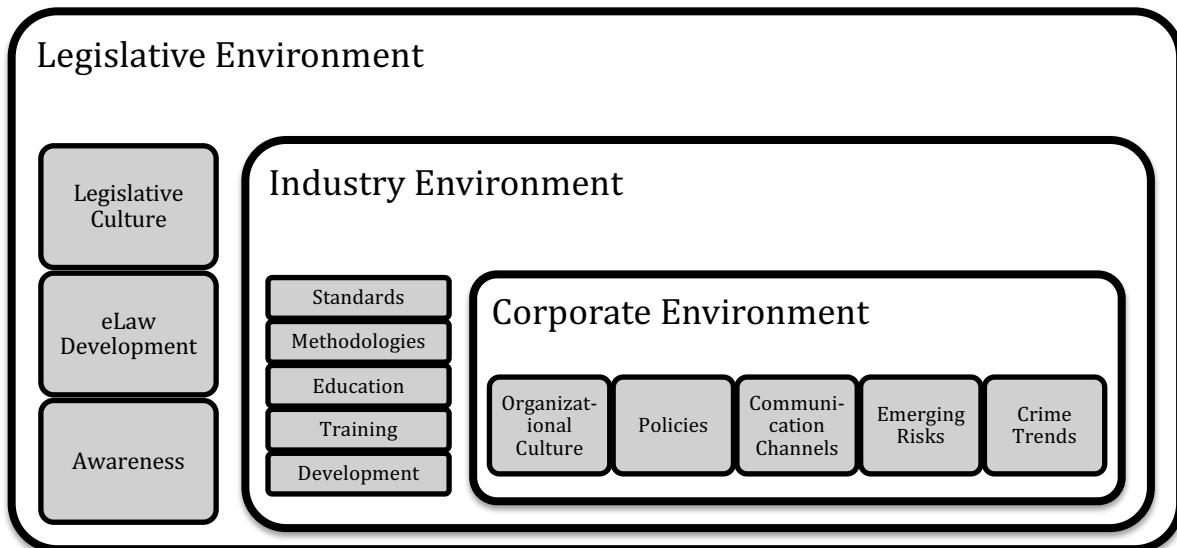


Figure 1. Cognitive Approaches for digital forensic readiness planning

The corporate environment has properties that are within an organisation's control that must be aligned with and support an organisation's digital forensic readiness plan. The corporate environment operates within the limitations of the industry environment, which, in turn, is influenced by the limitations of the legislative environment. A critical component of a digital forensic readiness plan is to establish a cooperation strategy that ensures that digital forensic cases can progress seamlessly from their inception in a corporate environment to conclusion in a court of law (legislative environment), following relevant guidelines in the industry environment to ensure that the integrity of evidence is maintained.

### 6. Conclusion

This study has sought to investigate cognitive approaches that aid in developing digital forensic readiness plans. The study reveals that developing a digital forensic readiness plan is a task that involves many factors beyond the realm of a single organisation. The factors are presented in the form of a conceptual model for organisations to use in process planning to achieve digital forensic readiness. By focusing on the lessons learned from experience, the study provides cognitive approaches to digital forensic readiness that can be used by

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

individuals who wish to explore this topic further as well as by organisations that desire to enhance their ability to respond to security incidents while maintaining the integrity of evidence and keeping investigative costs low.

Our future research will examine digital forensic readiness as it relates to specific contexts such as mobile devices, wireless networks, public key infrastructures and cloud computing.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**7. References**

- [1] ATLAS.ti Scientific Software Development, A world of data in your hand, Berlin, Germany ([www.atlasti.com](http://www.atlasti.com)).
- [2] M. Cohen, D. Bilby and G. Caronni, Distributed forensics and incident response in the enterprise, *Digital Investigation*, vol. 8(S), pp. S101-S110, 2011.
- [3] J. Corbin and A. Strauss, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Thousand Oaks, California, 2008.
- [4] J. Creswell and V. Clark, *Designing and Conducting Mixed Methods Research*, Sage Publications, Thousand Oaks, California, 2011.
- [5] S. Hoolachan and W. Glisson, Organisational handling of digital evidence, *Proceedings of the Conference on Digital Forensics, Security and Law*, pp. 33-44, 2010.
- [6] P. Kanellis, E. Kiountouzis, N. Kolokotronis and D. Martakos (Eds.), *Digital Crime and Forensic Science in Cyberspace*, Idea Group Publishing, Hershey, Pennsylvania, 2006.
- [7] Y. Manzano and A. Yasinsac, Policies to enhance computer and network forensics, *Proceedings of the Second Annual IEEE SMC Information Assurance Workshop*, pp. 289-295, 2001.
- [8] M. Patton, *Qualitative Research and Evaluation Methods*, Sage Publications, Thousand Oaks, California, 2002.
- [9] A. Poee and L. Labuschagne, A conceptual model for digital forensic readiness, *Proceedings of the South African Information Security Conference*, 2012.
- [10] Republic of South Africa, Electronic Communications and Transactions Act 2002, *Government Gazette*, vol. 446(2), no. 23708, August 2, 2002.
- [11] J. Salmons, *Online Interviews in Real Time*, Sage Publications, Thousand Oaks, California, 2010.
- [12] C. Teddlie and A. Tashakkori, *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*, Sage Publications, Thousand Oaks, California, 2009.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**Appendix 3: Interview Instrument**

---

	<b>Current Position:</b>		
	<b>Experience in digital forensics (years):</b>		
	<b>Company name &amp; contact details:</b>		
	<i>Introduce reason for research.</i>		
<b>2</b>	<b>BUILD RAPPORT</b>		
		<b>OBJECTIVE</b>	<b>CRITERIA</b>
	Over the years, what has been your involvement in digital crimes in South Africa?	Validate if interviewee meets minimum criteria	<ol style="list-style-type: none"> <li>1. Digital Forensics/Law</li> <li>2. Period &gt; 3 years</li> <li>3. Practiced in RSA</li> <li>4. Private/Public/Academic Sector</li> </ol>
<b>3</b>	<b>INTERVIEW QUESTIONS</b>	<b>OBJECTIVE</b>	<b>KEYWORD</b>
Q1	<i>Should South African organisations be concerned about digital crimes?</i>	Establish general attitude towards the effects of digital crimes.	<ol style="list-style-type: none"> <li>1. Material/Immaterial</li> <li>2. Damages</li> <li>3. Losses</li> <li>4. Impact</li> <li>5. Limitations</li> <li>6. Resources</li> <li>7. Major/Minor</li> </ol>
	<i>Yes/No: State reason:</i>		
Q2	Which three types of digital crimes do you find to be the most prevalent?	Establish the most prevalent types of DF crimes. Limit to top 3.	<ol style="list-style-type: none"> <li>1. Computer Based</li> <li>2. Online Based</li> <li>3. Cell Phone and other devices</li> </ol>

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Q3	Which sector do you find to be the most targeted?	Establish which sector and sub-sector is targeted the most. Using the standard industrial council subsector classification	<ol style="list-style-type: none"> <li>1. Private, Public or Parastatal</li> <li>2. Mining</li> <li>3. Manufacturing</li> <li>4. Electricity, Gas and Water</li> <li>5. Construction</li> <li>6. Retail, Motor Trade and Repair Services</li> <li>7. Wholesale Trade, Commercial Agents and Allied Services</li> <li>8. Catering, Accommodation and other Trade</li> <li>9. Transport, Storage and Communications</li> <li>10. Finance and Business Services</li> <li>11. Community, Social and Personal Services</li> <li>12. Agriculture</li> </ol>
Q4	Have you noted any challenges regarding the prosecution of digital crimes?	Establish prior challenges in respect of the specific sectors. Sector specific challenges/strengths	<ol style="list-style-type: none"> <li>1. Presence/Lack of</li> <li>2. Standard process</li> <li>3. Methodology</li> <li>4. Guidelines</li> <li>5. Best Practice</li> <li>6. Data Integrity</li> <li>7. Non-manipulation</li> <li>8. Repudiation</li> <li>9. Reliability</li> <li>10. Availability</li> <li>11. Accessibility</li> <li>12. People (Judge/Investigator)</li> <li>13. Training</li> <li>14. Reporting</li> <li>15. lack of knowledge/skill</li> </ol>
Q5	<i>Do you or your organisation have a digital forensic model that has been adopted?</i>	Establish if a formal digital model is used and how it's applied.	<ol style="list-style-type: none"> <li>1. DF model name</li> <li>2. Strengths/Weaknesses</li> </ol>
Q6	<i>Does electronic evidence provide sufficient assurance of non-manipulation?</i>	Establish if DF process maintains data integrity	<ol style="list-style-type: none"> <li>1. Data Integrity</li> <li>2. Non-manipulation</li> <li>3. Repudiation</li> <li>4. Reliability</li> <li>5. Availability</li> <li>6. Accessibility</li> </ol>
Q7	<i>Is there a standard process for electronic evidence gathering?</i>	Establish if common standard exists	<ol style="list-style-type: none"> <li>1. Yes, motivate</li> <li>2. No, motivate</li> </ol>


**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Q8	<i>Does the law adequately position the acceptable use of/or extent to which electronic evidence can be used in a civil or criminal proceedings?</i>	Are there guidelines on what the courts will accept regarding e-evidence	1. Yes, motivate 2. No, motivate
Q9	<i>Does the law cater to the complexities of modern IT devices?</i>	Identify challenges with the law	1. Yes, motivate 2. No, motivate
Q10	<i>What are the factors that contribute to electronic evidence being rendered inadmissible?</i>	Identify challenges with the process	1. Yes, motivate 2. No, motivate
Q11	<i>Have you noted any challenges that prevent digital crime investigators from correctly applying the digital forensic model or framework?</i>	Identify challenges with the model	1. Yes, motivate 2. No, motivate
Q12	<i>Do you think digital forensic investigators are sufficiently trained to do their work?</i>	Identify challenges with the people	1. Diploma 2. Degree 3. Certificate 4. Special Course 5. Internal/External Course 6. Informal/Formal training 7. Regular/Once-off
Q13	<i>Have you noted any challenges that prevent prosecutors from successfully prosecuting digital crimes?</i>	Identify challenges with the people	1. Practicality of Model 2. Process challenges 3. Internal/External 4. Technical 5. Legal 6. Awareness/Knowledge 7. Resources 8. Pressures
Q14	<i>Do you think state prosecutors are sufficiently trained to do their work?</i>	Identify challenges with the people	1. Yes, motivate 2. No, motivate
Q15	<i>What do you think should be done to increase the prosecution rate of digital crimes in South Africa?</i>	Establish general perceptions on what can be done as part of the solution.	1. People 2. Process 3. Technology (HW/SW) 4. Law 5. Report cases 6. Evidence

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**Appendix 4: Interview Consent Letter**

---



**LETTER OF CONSENT**

I \_\_\_\_\_

(ID: \_\_\_\_\_) agree to voluntarily participate in the research to develop a multi-disciplinary digital forensic model for the South African Law enforcement, conducted by Antonio Poee through the University of South Africa.

I have been informed of and agree to the following:

1. My identity will be kept anonymous;
2. The name of my organization will be kept anonymous;
3. I am free to withdraw from this research at any time without negative or undesirable consequences to me or my organization;
4. I understand that the information provided will be used for research purposes only; and
5. It is my responsibility to obtain permission/clearance from my organization to participate in this research.

1

Open Rubric

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

The information provided in given in my capacity as (Job Title)

---

**Student Researcher**

Name: Antonio Poee

Signature: 

Email: [\\_antonio.poee@gmail.com](mailto:_antonio.poee@gmail.com)

Tel: \_\_072 781 4157\_\_\_\_\_

**Supervisor**

Name: Prof Les Labuschagne

Signature: 

Email: [labus@unisa.ac.za](mailto:labus@unisa.ac.za)

Tel: \_\_012 429 6368\_\_\_\_\_

**Interviewee**

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Email: \_\_\_\_\_

Email: \_\_\_\_\_



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**



Dear Participant,

**INTERVIEW: DEVELOPING A MULTI-DISCIPLINARY DIGITAL FORENSIC MODEL FOR SOUTH  
AFRICAN LAW ENFORCEMENT: A MIXED METHOD STUDY**

Thank you for your interest in participating in this PhD research project on Digital Forensic Models undertaken in the School of Computing at the University of South Africa.

This study will investigate the factors contributing to the low prosecution rate for digital crimes in the South African courts. This will involve a literature survey, interviews and action research. The purpose of this three-phase, exploratory sequential design will be to develop a digital forensic methodology specific to the South African context, and how this can be used to increase the prosecution rate for computer crimes in the said context.

The following information will give you more details regarding your interview.

Who are the researchers?

The study is presently being carried out by Mr Antonio Pooe, as part of his PhD Information Systems degree under supervision of Prof Les Labuschagne (Director: School of Computing) from the University of South Africa.

What do we expect from you in the study:

Participation in this interview is voluntary. By taking part in the interview, you agree to take part in this research and to the publication of the anonymous results with the understanding that individual and company anonymity will be preserved. If at any stage you do not wish to continue with the interview, you may withdraw your consent.

The interview will take you, at most 45 minutes to complete.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

How are we going to use the results?

This is an anonymous study. The results of the project will be published as part of a thesis and/or an article/s, but you may be assured that any identifying information obtained in connection with this study will remain confidential and will not be disclosed.

What are we doing to ensure confidentiality?

To ensure data confidentiality, electronic data is kept on an encrypted drive of the researchers computer. Access to the said computer is also limited to the researcher. Furthermore, all hard copy documents are stored in a locked cabinet at the residence of the researcher. Access to the cabinet is also restricted.

If at any stage you have any queries or concerns regarding your participation in this study, please contact us.

Thank you for your participation.

Best Regards,



Prof Les Labuschagne

Director: School of Computing

Tel: (012) 429 6368

Email: [llabus@unisa.ac.za](mailto:llabus@unisa.ac.za)



---

Antonio Pooc

Student Researcher

Tel: 072 781 4157

Email: [Antonio.pooc@gmail.com](mailto:Antonio.pooc@gmail.com)

## **Appendix 5: Case Study 1: Atlas.ti Coding Summary Report**

---

List of all objects

---

**HU**

---

Case Law - Verification Chapter

### **Primary Documents**

---

P 1: Case Law - Verification.rtf {424}

### **Quotations**

---

1:1 British American Tobacco Compa.. (35:35)  
1:2 Rawsonville in the Western Cap.. (35:35)  
1:3 West Coast road near Darling (35:35)  
1:4 Kinkelbos, outside Port Elizab.. (35:35)  
1:5 common law offences of theft, .. (39:39)  
1:6 Rawsonville, Darling and Kinke.. (39:39)  
1:7 Lenasia South, Vereeniging (39:39)  
1:8 Kinkelbos (39:39)  
1:9 Firearms Control Act, 60 of 20.. (41:41)  
1:10 Prevention of Organised Crime .. (41:41)  
1:11 trial lasting more than 160 co.. (55:55)  
1:12 State alone led the evidence (55:55)  
1:13 90 witnesses (55:55)  
1:14 testified on their own behalf (55:55)  
1:15 evidence of the s 204 (59:59)  
1:16 records of the cell phone acti.. (59:59)  
1:17 State sought to demonstrate (59:59)  
1:18 cell phone records (59:59)  
1:19 corroborate his evidence and s.. (59:59)  
1:20 cell phone evidence (59:59)  
1:21 introduce the cell phone recor.. (59:59)  
1:22 cell phone evidence (59:59)  
1:23 trials-within-a-trial (59:59)  
1:24 trials-within-a-trial (59:59)  
1:25 admissibility of exhibits seiz.. (59:59)  
1:26 police (59:59)  
1:27 police search and seizure oper.. (59:59)  
1:28 one or more cell phones were s.. (59:59)  
1:29 link (59:59)  
1:30 records of cell phone activity.. (59:59)  
1:31 linking (59:59)  
1:32 State sought, furthermore, to .. (59:59)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:33 linkages (59:59)  
1:34 information downloaded from th.. (59:59)  
1:35 seized (59:59)  
1:36 seized certain other articles (59:59)  
1:37 State led the evidence (59:59)  
1:38 one or more drivers or assista.. (59:59)  
1:39 cell phone evidence (61:61)  
1:40 jurisdiction of this Court in .. (64:64)  
1:41 last two robberies in the East.. (64:64)  
1:42 Seven accused hail from Ennerd.. (64:64)  
1:43 Firearms Control Act, counts 2.. (64:64)  
1:44 Soweto (64:64)  
1:45 s 2(4) of POCA (64:64)  
1:46 National Director of Public Pr.. (64:64)  
1:47 POCA (64:64)  
1:48 s 111 of Act 51 of 1977 (66:66)  
1:49 proceedings against the accuse.. (66:66)  
1:50 Mr. Vernon Aspelng was called.. (69:69)  
1:51 at the request of the prosecut.. (69:69)  
1:52 answer all questions fully and.. (69:69)  
1:53 he has been in a witness prote.. (71:71)  
1:54 Vernie's Transport (71:71)  
1:55 Rawsonville (73:73)  
1:56 Cape Town (73:73)  
1:57 Waterfront Suites in Green Poi.. (73:73)  
1:58 mid-Ennerdale (77:77)  
1:59 Cape Town (77:77)  
1:60 Waterfront Suites (77:77)  
1:61 Johannesburg (83:83)  
1:62 Cape Town (83:83)  
1:63 Cape Town (83:83)  
1:64 Cape Town (83:83)  
1:65 other countries in Africa (83:83)  
1:66 sketched his knowledge (85:85)  
1:67 taxi rank in Ennerdale (88:88)  
1:68 Ultra City in Bloemfontein (92:92)  
1:69 Cape Town (92:92)  
1:70 Three Sisters (92:92)  
1:71 Waterfront Suites in Green Poi.. (92:92)  
1:72 cigarette company (94:94)  
1:73 Cape Town (94:94)  
1:74 Montague Gardens (96:96)  
1:75 BATSA's (96:96)  
1:76 Green Point (96:96)  
1:77 BATSA (98:98)  
1:78 BATSA (98:98)  
1:79 BATSA (98:98)  
1:80 BATSA (98:98)  
1:81 Worcester (98:98)  
1:82 Robertson (100:100)  
1:83 BATSA (100:100)  
1:84 BATSA (100:100)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:85 BATSA (100:100)  
1:86 Waterfront Suites in Green Poi.. (100:100)  
1:87 Ennerdale (100:100)  
1:88 Lenasia (102:102)  
1:89 Bera's Transport (102:102)  
1:90 Cape Town (104:104)  
1:91 Cape Town (104:104)  
1:92 Cape Town (108:108)  
1:93 Cape Town (108:108)  
1:94 Engen truck stop en route to M.. (110:110)  
1:95 Waterfront Suites (112:112)  
1:96 Cape Town (112:112)  
1:97 Johannesburg (114:114)  
1:98 Cape (114:114)  
1:99 Montague Gardens (118:118)  
1:100 Waterfront Suites (118:118)  
1:101 Montague Gardens (118:118)  
1:102 Malmesbury road (118:118)  
1:103 BATSA (118:118)  
1:104 BATSA (118:118)  
1:105 BATSA (118:118)  
1:106 Gauteng (120:120)  
1:107 Bera's Transport (122:122)  
1:108 Ennerdale (122:122)  
1:109 Port Elizabeth (125:125)  
1:110 Gauteng (125:125)  
1:111 Port Elizabeth (125:125)  
1:112 East London. (125:125)  
1:113 Port Elizabeth (125:125)  
1:114 Port Elizabeth (125:125)  
1:115 Port Elizabeth (125:125)  
1:116 Grahamstown (125:125)  
1:117 Port Elizabeth (125:125)  
1:118 Cape Town (127:127)  
1:119 Bera's Transport (127:127)  
1:120 Bera's Transport (127:127)  
1:121 Kroonvaal Toll Plaza (127:127)  
1:122 Colesberg (127:127)  
1:123 Ennerdale (127:127)  
1:124 Port Elizabeth (129:129)  
1:125 Cape Town (129:129)  
1:126 Port Elizabeth (129:129)  
1:127 Formula 1 hotel in Alberton (137:137)  
1:128 Lenasia (143:143)  
1:129 Ennerdale (143:143)  
1:130 affidavits (165:165)  
1:131 Aspelings three affidavit (165:165)  
1:132 minor discrepancies in his/her.. (165:165)  
1:133 searched (173:173)  
1:134 s 208 of the Criminal Procedur.. (232:232)  
1:135 two s 205 subpoenas (264:264)  
1:136 Vodacom (264:264)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:137 prosecutor or investigating of.. (264:264)
- 1:138 Detailed billing records (265:265)
- 1:139 Ms Petro Heynecke (264:264)
- 1:140 Ms Hilda du Plessis (274:274)
- 1:141 MTN (274:274)
- 1:142 Detailed billing records (275:275)
- 1:143 "It is requested that it be es.. (281:281)
- 1:144 Ms Hilda du Plessi (286:286)
- 1:145 MTN (286:286)
- 1:146 testified (286:286)
- 1:147 forensic data analyst (286:286)
- 1:148 access (286:286)
- 1:149 MTN's database (286:286)
- 1:150 only person (286:286)
- 1:151 forensic requests for access t.. (286:286)
- 1:152 witness testified (286:286)
- 1:153 MTN (286:286)
- 1:154 South African Police Services (286:286)
- 1:155 cell phone data in terms s 205.. (286:286)
- 1:156 electronic format and cannot b.. (286:286)
- 1:157 no such manipulation takes pla.. (286:286)
- 1:158 MTN (286:286)
- 1:159 kept in a back-up system in th.. (286:286)
- 1:160 subpoena (288:288)
- 1:161 MTN (288:288)
- 1:162 MTN's computerized database (288:288)
- 1:163 State seeks to link (288:288)
- 1:164 State (288:288)
- 1:165 Telematrix (288:288)
- 1:166 link (288:288)
- 1:167 link (288:288)
- 1:168 link (288:288)
- 1:169 cross-examination (290:290)
- 1:170 authenticity (290:290)
- 1:171 Mr. Cornelius Basson (290:290)
- 1:172 MTN (290:290)
- 1:173 responsible (290:290)
- 1:174 operation of the systems which.. (290:290)
- 1:175 operating systems are pre-test.. (290:290)
- 1:176 properly maintained (290:290)
- 1:177 very high level of reliability.. (290:290)
- 1:178 Ms Petro Heynecke (292:292)
- 1:179 Vodacom (292:292)
- 1:180 testify (292:292)
- 1:181 forensic liaison manager at Vo.. (292:292)
- 1:182 Vodacom systems (292:292)
- 1:183 The Vodacom systems hold the h.. (292:292)
- 1:184 The witness's attention was di.. (294:294)
- 1:185 The witness's main responsibil.. (296:296)
- 1:186 released in the encrypted port.. (296:296)
- 1:187 tampered (296:296)
- 1:188 police (296:296)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:189 link (298:298)  
1:190 testified (298:298)  
1:191 link (298:298)  
1:192 link (300:300)  
1:193 link (302:302)  
1:194 cell phone documentation (302:302)  
1:195 Vodacom documentation (302:302)  
1:196 link (302:302)  
1:197 Vodacom documentation (302:302)  
1:198 identified (302:302)  
1:199 witness testified (304:304)  
1:200 The data was never tampered wi.. (304:304)  
1:201 designed in accordance with a .. (304:304)  
1:202 data was received from the arc.. (304:304)  
1:203 Mr. Jasper Smi (306:306)  
1:204 Vodacom (306:306)  
1:205 testified (306:306)  
1:206 responsible (306:306)  
1:207 integrity of Vodacom's systems.. (306:306)  
1:208 had experienced no problems in.. (306:306)  
1:209 kept in the system for a perio.. (306:306)  
1:210 retained (306:306)  
1:211 number of years in Vodacom's a.. (306:306)  
1:212 Mr. Spangenberg (308:308)  
1:213 criminal proceeding (308:308)  
1:214 s 15(4) of the Electronic Comm.. (308:308)  
1:215 cell phone documentation had n.. (315:315)  
1:216 Uniform Rule 54(5) (315:315)  
1:217 Registrar of the High Court. (315:315)  
1:218 s 205 of Act 51 of 1977 (315:315)  
1:219 The subpoenas are counter-sign.. (315:315)  
1:220 s 59 of The Regulation of Inte.. (319:319)  
1:221 carries significant evidenti.. (323:323)  
1:222 Further, in my view, subject t.. (323:323)  
1:223 Further, in my view, subject t.. (323:323)  
1:224 police (343:343)  
1:225 testified (343:343)  
1:226 cell phones seized (343:343)  
1:227 evidence was that the cellular.. (343:343)  
1:228 sealed forensic bag (343:343)  
1:229 sealed (343:343)  
1:230 arresting officers (343:343)  
1:231 recorded (343:343)  
1:232 match (343:343)  
1:233 link (343:343)  
1:234 reliability and accuracy of th.. (345:345)  
1:235 lack of technical competency o.. (345:345)  
1:236 cross-examination (347:347)  
1:237 police (347:347)  
1:238 witnesses (347:347)  
1:239 testified (347:347)  
1:240 volume and complexity of the c.. (347:347)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:241 cell phone evidence (349:349)
- 1:242 linkages (349:349)
- 1:243 State led the evidence (349:349)
- 1:244 expert (349:349)
- 1:245 combining the data (349:349)
- 1:246 He linked calls and linked the.. (349:349)
- 1:247 modus operandi (37:37)
- 1:248 In each case the modus operand.. (37:37)
- 1:249 On 24 June 2003 a truck carryi.. (35:35)
- 1:250 Whilst the bulk of the charges.. (39:39)
- 1:251 After flagging down the BATSA .. (37:37)
- 1:252 As far as statutory offences a.. (41:41)
- 1:253 Count 1 alleged that several o.. (43:43)
- 1:254 Ultimately accused number 1 an.. (53:53)
- 1:255 In a trial lasting more than 1.. (55:55)
- 1:256 called witnesses (55:55)
- 1:257 Accused 2, 3, 6, 7, 10 and 11 .. (55:55)
- 1:258 The chief pillar of the State'.. (59:59)
- 1:259 corroborate his evidence and s.. (59:59)
- 1:260 police search and seizure oper.. (59:59)
- 1:261 strengthen such linkages by in.. (59:59)
- 1:262 I propose to deal with the two.. (61:61)
- 1:263 The State thus commenced its p.. (64:64)
- 1:264 A further document handed up a.. (66:66)
- 1:265 State's principal witness (69:69)
- 1:266 Ever since that time he has be.. (71:71)
- 1:267 By 2003 it appears that he had.. (71:71)
- 1:268 Accused 2 was the younger brot.. (73:73)
- 1:269 The witness had known accused .. (79:79)
- 1:270 As the evidence revealed the e.. (83:83)
- 1:271 About a month before the first.. (88:88)
- 1:272 The following day Zallie calle.. (90:90)
- 1:273 [25] On Monday, 23 June 2003 a.. (95:96)
- 1:274 [52] On or about 7 November 20.. (152:153)
- 1:275 The State tendered in evidence.. (175:175)
- 1:276 Van Rooyen's evidence was not .. (177:177)
- 1:277 The admissibility of that evid.. (185:185)
- 1:278 Aspelng's evidence was extens.. (187:187)
- 1:279 He was, as was put to him on s.. (195:195)
- 1:280 Notwithstanding these criticis.. (197:197)
- 1:281 He continued to answer all oth.. (199:199)
- 1:282 It is trite law, however, that.. (207:223)
- 1:283 The Court will bear in mind th.. (237:237)
- 1:284 That evidence was contested at.. (239:239)
- 1:285 phones allegedly used by, inte.. (59:59)
- 1:286 records (59:59)
- 1:287 The cell phone evidence was co.. (59:59)
- 1:288 were seized from each accused'.. (59:59)
- 1:289 witness protection programme (71:71)
- 1:290 witness (73:73)
- 1:291 witness (75:75)
- 1:292 witness (77:77)



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:293 Aspeling identified accused (81:81)  
1:294 . Aspeling also testified that.. (85:85)  
1:295 Returning to Aspeling's eviden.. (116:116)  
1:296 ] Nonetheless Aspeling believe.. (131:131)  
1:297 Accused 3 called him, saying: .. (133:133)  
1:298 The route which Aspeling follo.. (135:135)  
1:299 [46] The witness drove into Fr.. (140:141)  
1:300 Aspeling, accused 7 and Grant .. (145:145)  
1:301 Accused 7 urged Aspeling and o.. (147:149)  
1:302 ] On the Saturday evening they.. (151:151)  
1:303 After his appearance in the Ma.. (155:155)  
1:304 ide range of exhibits by the p.. (155:155)  
1:305 exhibits (155:155)  
1:306 photographs (155:155)  
1:307 photographs (155:155)  
1:308 extract from a docket (155:155)  
1:309 cell phone numbers and names d.. (155:155)  
1:310 his cell phone record (155:155)  
1:311 extracts from the documents pu.. (155:155)  
1:312 evidence in chief given by Asp.. (157:157)  
1:313 These included that Aspeling w.. (157:157)  
1:314 ] Instead, it was put to him, .. (159:159)  
1:315 He was probed, time and again,.. (161:161)  
1:316 [57] Another area which attrac.. (162:163)  
1:317 . Secondly, Aspeling's own exp.. (165:165)  
1:318 s 204 witness (165:165)  
1:319 It was not the purpose of such.. (165:165)  
1:320 evidence were confirmed or cor.. (167:167)  
1:321 testified (167:167)  
1:322 During this trip accused 2 had.. (169:169)  
1:323 He confirmed too that after fo.. (171:171)  
1:324 testified (171:171)  
1:325 Aspeling testified hearing tha.. (173:173)  
1:326 State led the evidence (173:173)  
1:327 (exhibit "W" (173:173)  
1:328 exhibit "X (173:173)  
1:329 testifying that he had no know.. (173:173)  
1:330 State tendered in evidence cop.. (175:175)  
1:331 Aspeling explained that the in.. (175:175)  
1:332 Aspeling testified that shortl.. (177:177)  
1:333 cross-examination (177:177)  
1:334 Hall testified that this perso.. (179:179)  
1:335 A warning statement made by ac.. (179:179)  
1:336 The proliferation of exhibits .. (179:179)  
1:337 the officer in overall charge .. (181:181)  
1:338 In the vehicle's cubby-hole he.. (181:181)  
1:339 There a telephone number attri.. (181:181)  
1:340 On 14 October 2003 Inspector H.. (183:183)  
1:341 Mr. Vincent Matthysen, as well.. (183:183)  
1:342 an orange and yellow reflectiv.. (183:183)  
1:343 bullet proof jacket but with n.. (183:183)  
1:344 d (183:183)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:345 reflective jacket was also ide.. (183:183)
- 1:346 evidence lies in the voluminou.. (185:185)
- 1:347 own cell phone data, and that .. (185:185)
- 1:348 evidence was extensively criti.. (187:187)
- 1:349 he repeatedly contradicted his.. (187:187)
- 1:350 Aspeling's evidence was also c.. (189:189)
- 1:351 As far as another major area o.. (191:191)
- 1:352 Aspeling testified over an ext.. (193:193)
- 1:353 Aspeling testified in extraord.. (193:193)
- 1:354 his evidence in chief was deli.. (193:193)
- 1:355 He was, as was put to him on s.. (195:195)
- 1:356 Notwithstanding these criticis.. (197:197)
- 1:357 Aspeling appeared to enjoy the.. (197:197)
- 1:358 his tendency to sometimes beco.. (197:197)
- 1:359 to ask the cross-examiner ques.. (197:197)
- 1:360 Aspeling's failure to answer a.. (197:197)
- 1:361 The cross-examination in quest.. (197:197)
- 1:362 Its tone was evidenced by Stat.. (197:197)
- 1:363 Aspeling declined to answer fu.. (199:199)
- 1:364 Aspeling immediately declared .. (199:199)
- 1:365 Notwithstanding the extremely .. (201:201)
- 1:366 This explanation cannot be rej.. (201:201)
- 1:367 Aspeling impressed as someone .. (203:203)
- 1:368 He revealed himself as someone.. (203:203)
- 1:369 although not flawless, contain.. (205:205)
- 1:370 State relied heavily on docume.. (239:239)
- 1:371 What I will refer to generally.. (241:241)
- 1:372 admissibility of articles seiz.. (241:241)
- 1:373 two cell phones as well as doc.. (253:253)
- 1:374 two cell phones (254:254)
- 1:375 black plastic bag containing v.. (254:254)
- 1:376 a cell phone (255:255)
- 1:377 white Volkswagen Golf ; (255:255)
- 1:378 a white Volkswagen Polo, a whi.. (257:257)
- 1:379 two cell phones and documentat.. (257:257)
- 1:380 Those records were similarly o.. (259:259)
- 1:381 Detailed billing records (265:265)
- 1:382 including calls made and recei.. (265:265)
- 1:383 Detailed billing records perta.. (275:275)
- 1:384 including calls made and recei.. (275:275)
- 1:385 MTN personnel worked after hou.. (288:288)
- 1:386 . Du Plessis identified exhibi.. (288:288)
- 1:387 The witness then identified ex.. (288:288)
- 1:388 In cross-examination it was pu.. (290:290)
- 1:389 authenticity of the documentat.. (290:290)
- 1:390 He added that the systems invo.. (290:290)
- 1:391 He stated that the operating s.. (290:290)
- 1:392 received internal training in .. (292:292)
- 1:393 The Vodacom systems hold the h.. (292:292)
- 1:394 The data contains all cell pho.. (292:292)
- 1:395 It contains both successful an.. (292:292)
- 1:396 The witness's attention was di.. (294:294)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:397 The first column contains the .. (294:294)
- 1:398 Only once the data is moved fr.. (296:296)
- 1:399 Only once the data is moved fr.. (296:296)
- 1:400 The data is processed in masse.. (296:296)
- 1:401 Since Vodacom receives many su.. (296:296)
- 1:402 Vodacom cannot change one set .. (296:296)
- 1:403 The witness then had her atten.. (298:298)
- 1:404 Ms Heyneke identified exhibit .. (300:300)
- 1:405 State sought to link to accuse.. (302:302)
- 1:406 State sought to link to accuse.. (302:302)
- 1:407 State sought to link to accuse.. (302:302)
- 1:408 applicable to the cell phone d.. (313:313)
- 1:409 having to call a witness to pr.. (313:313)
- 1:410 In my view the evidence of Mes.. (313:313)
- 1:411 The reference by counsel to un.. (317:317)
- 1:412 Cell phone numbers connected t.. (331:331)
- 1:413 Henry Cottle, a security offic.. (331:331)
- 1:414 entoor explained that he had a.. (331:332)
- 1:415 Speed was also involved in exe.. (333:333)
- 1:416 he downloaded the following re.. (333:333)
- 1:417 Aspeling testified that the ce.. (336:336)
- 1:418 Analysis of the Vodacom data i.. (338:338)
- 1:419 An analysis of the MTN cell ph.. (340:340)
- 1:420 One example was an instance wh.. (345:345)
- 1:421 police witnesses (347:347)
- 1:422 exhibits seized by the police (59:59)
- 1:423 police officers testified (343:343)
- 1:424 police requested the data to b.. (296:296)

**Codes**

---

\ {0-0}

Analysis (IE5) {16-1}~

Comment:

Analysis of evidence and its attributes.

Case Law {1-0}~

Comment:

Consider case law in preparation

CE {28-0}~

Comment:

establish domain

Collection (IE2) {24-3}~

Comment:

Correct method/tools to collect evidence without compromising forensic integrity.

Criminal Process (LE2) {16-6}~

Comment:

Correct application of the Criminal Process in ensuring evidence discovery, maintaining integrity of evidence seized, and adherence to due process.

DFR Technologies (CE5) {20-2}~

Comment:

Digital Forensic Ready technology to maintain forensic attributes in all data stored.

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Documentation (IE7) {4-1}~

Comment:

Thorough documentation and chain of custody relating to the case.

Electronic Laws (LE1) {21-3}~

Comment:

Comprehensive legislation detailing compliance specifications

Evidence: Corroborative / Nature {4-0}~

Comment:

Consider nature of evidence and supportive/corroborative evidence.

Documentary vs Real evidence

Evidence: Testing {1-0}

Evidentiary: Value {2-0}~

Comment:

Careful scrutiny of evidence and correct interpretation of findings.

Consider the weight of the evidence obtained.

Human Resources (CE4) {27-4}~

Comment:

Ability to operate forensic ready technology, and provide expert witness.

Identification (IE4) {6-1}~

Comment:

Identification of key evidence attributes for analysis.

Interpretation (IE6) {19-2}~

Comment:

Correct interpretation of findings during investigation and analysis stage.

Investigation: Methodology {2-0}~

Comment:

Determine investigative approach and methodology

Stick to the plan.

Investigation: Scope {1-0}~

Comment:

after modus operandi, establish limitations and set investigation scope

Jurisdiction {67-0}~

Comment:

establish legal jurisdiction (geographic location and relevant laws)

consider laws as per country, state, province, city, town etc.

Justice Personnel (LE5) {11-1}~

Comment:

Correct interpretation of digital forensic results during prosecution stage.

Justice System (LE3) {7-10}~

Comment:

Ability to interpret and prosecute cases involving electronic evidence.

Law Enforcement Agents (LE4) {10-1}~

Comment:

Knowledge and willingness to investigate e-crimes.

Legal Charges {1-0}~

Comment:

Consider charges as per contravened laws (federal or state law)

Legislative Scope {1-0}~

Comment:

Define legal contraventions.

Limitations: Legal {2-0}

Maturity of the legal system {1-0}~

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Comment:

Principle of fairness  
modus operandi {1-0}~

Comment:

Establish the what/how/who/when/why etc. of the incident.  
nature of crimes {1-0}~

Comment:

determine the nature of offenses as per laws in that jurisdiction  
Policies (CE2) {8-2}~

Comment:

Organisation to develop policies that govern forensic readiness.  
Presentation (IE8) {56-8}~

Comment:

Demonstration/Application of education, training and certification of CIRT/Witnesses on  
presentation of evidence.

Preservation (IE1) {19-3}~

Comment:

Evidence preserved in accordance with industry standards and aligned to legislative  
requirements.

Procedures (CE3) {11-2}~

Comment:

Organisation to develop procedures that govern forensic readiness.

Resources: Law Enforcement {1-0}~

Comment:

Availability and competence of police.

Resources: Legal Representation {1-0}~

Comment:

Consider availability of competent legal representation.

Resources: Suspects {1-0}

Resources: Timeline {1-0}

Resources: Witnesses {10-0}~

Comment:

Consider key/principal witness/es  
Consider value of witnesses.  
Protection of witness.  
Integrity.  
Credibility.  
Expertise & Experience.  
Relationship between witnesses/accused.  
Preparation of witness for court.

Retention (IE9) {2-1}~

Comment:

Retention of evidence as required by law.

Standards (CE1) {3-2}~

Comment:

Organisational standards developed in harmony with legislative requirements.

Synopsis {17-0}~

Comment:

what transpired?  
obtain all facts?  
sequence of events? timeline.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

Validation (IE3) {8-1}~

Comment:

Validating evidence for relevance and corroboration.

### Code Families

---

Corporate Environment (6)

Industry Environment (9)

Legislative Environment (5)

### Network Views

---

E-Crime Prosecution LE4 | IE8 (2)

Evidence Collection IE2 | LE2 (2)

Evidence Handling CE4 | LE3 | IE2 (3)

Evidence Preservation - CE5 | IE1 | LE2 (3)

Justice System Implementation LE5 | IE6 (2)

M-DiFoRe Network Links (19)

Methodology Evaluation LE3 - IE1 to IE9 (10)

Policy Alignment CE2 | IE8 | LE1 (3)

Procedural Implementation IE8 | CE3 | LE2 (3)

Standards Localisation IE8 | CE1 | LE1 (3)

Witness Preparation CE4 | IE8 | LE2 (3)

### Code-Links

---

Collection (IE2) <comply with> Criminal Process (LE2)

Criminal Process (LE2) <is associated with> Preservation (IE1)

DFR Technologies (CE5) <comply with> Criminal Process (LE2)

DFR Technologies (CE5) <must achieve> Preservation (IE1)

Human Resources (CE4) <comply with> Collection (IE2)

Human Resources (CE4) <comply with> Criminal Process (LE2)

Human Resources (CE4) <Cooperate with> Justice System (LE3)

Human Resources (CE4) <must achieve> Presentation (IE8)

Justice Personnel (LE5) <is associated with> Interpretation (IE6)

Justice System (LE3) <comply with> Analysis (IE5)

Justice System (LE3) <comply with> Collection (IE2)

Justice System (LE3) <comply with> Documentation (IE7)

Justice System (LE3) <comply with> Identification (IE4)

Justice System (LE3) <comply with> Interpretation (IE6)

Justice System (LE3) <comply with> Presentation (IE8)

Justice System (LE3) <comply with> Preservation (IE1)

Justice System (LE3) <comply with> Retention (IE9)

Justice System (LE3) <comply with> Validation (IE3)

Law Enforcement Agents (LE4) <comply with> Presentation (IE8)

Policies (CE2) <comply with> Electronic Laws (LE1)

Policies (CE2) <comply with> Presentation (IE8)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Presentation (IE8) <comply with> Criminal Process (LE2)  
Presentation (IE8) <comply with> Electronic Laws (LE1)  
Presentation (IE8) <comply with> Procedures (CE3)  
Presentation (IE8) <comply with> Standards (CE1)  
Procedures (CE3) <is property of> Criminal Process (LE2)  
Standards (CE1) <is property of> Electronic Laws (LE1)

## Appendix 6: Case Study 2: Atlas.ti Coding Summary Report

---

List of all objects

---

HU

---

Case Verification - Accepted Evidence 2

**Primary Doc**

---

P 1: 926.rtf {168}

**Quotations**

---

1:1 I heard evidence for some thre.. (83:83)  
1:2 Various lengthy affidavits wer.. (83:83)  
1:3 during the course of the proce.. (83:83)  
1:4 but having been given the nece.. (83:83)  
1:5 was able to conduct his defenc.. (83:83)  
1:6 I am completely satisfied that.. (83:83)  
1:7 He was told that he need not p.. (83:83)  
1:8 emanate to a large extent from.. (87:87)  
1:9 The First Plaintiff has a divi.. (87:87)  
1:10 Second Plaintiff is the Managi.. (87:87)  
1:11 This industry is a notoriously.. (87:87)  
1:12 It enters into Service Level A.. (90:90)  
1:13 it guarantees to meet minimum .. (90:90)  
1:14 It has about 500 skilled techn.. (90:90)  
1:15 The information derived from t.. (90:90)  
1:16 such service level standards r.. (90:90)  
1:17 If Bytes MS drops below the ag.. (91:91)  
1:18 it is typically given a month .. (91:91)  
1:19 it may also face effective fin.. (91:91)  
1:20 Second Plaintiff and the facts.. (97:97)  
1:21 Bytes MS' clients, rely on a g.. (97:97)  
1:22 effective and efficient runnin.. (97:97)  
1:23 is entrusted to the support an.. (97:97)  
1:24 it is a business imperative fo.. (97:97)  
1:25 its reputation for integrity, .. (97:97)  
1:26 The Second Plaintiff testified.. (97:97)  
1:27 He was employed in Bytes MS as.. (101:101)  
1:28 He had to attend weekly execut.. (101:101)  
1:29 5.1 Executive and other commit.. (102:110)  
1:30 Because the scope and type of .. (113:113)  
1:31 13.2 of the Defendant's standa.. (113:116)  
1:32 Confidential information, whic.. (122:122)



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:33 To that end, Defendant who was.. (124:124)  
1:34 Not to reveal confidential inf.. (126:126)  
1:35 Not to interfere with or endea.. (128:128)  
1:36 Not to “persuade, induce, soli.. (132:132)  
1:37 Not to use any confidential in.. (134:134)  
1:38 To surrender all confidential .. (136:137)  
1:39 evidence was that Defendant’s .. (140:140)  
1:40 16 March 2009 Defendant referr.. (140:140)  
1:41 Defendant was grossly negligen.. (140:140)  
1:42 He denied any wrong doing and .. (140:140)  
1:43 This application was dismissed.. (140:140)  
1:44 9. I will deal with certain fa.. (142:143)  
1:45 “As stated in my previous e-ma.. (143:143)  
1:46 Bytes MS had allegedly been de.. (148:148)  
1:47 The Defendant allegedly attemp.. (150:151)  
1:48 The identity of Bytes MS clien.. (151:151)  
1:49 On 16 October 2009 Defendant’s.. (154:154)  
1:50 Second Plaintiff had testified.. (154:154)  
1:51 Second Plaintiff also testifie.. (154:154)  
1:52 These e-mails are almost ident.. (158:158)  
1:53 He also told the recipients th.. (158:158)  
1:54 Also, on 25 November 2009 Defe.. (159:159)  
1:55 This e-mail to Kagiso was forw.. (162:162)  
1:56 As a result Plaintiffs’ Attorn.. (165:165)  
1:57 I may add that Defendant did n.. (166:166)  
1:58 On this day Defendant sent an .. (170:170)  
1:59 I will quote a part of this em.. (171:173)  
1:60 the Plaintiffs launched an urg.. (175:175)  
1:61 “The SCCU investigating office.. (173:173)  
1:62 Pending the outcome of an acti.. (175:175)  
1:63 On 23 December 2009 Sapire AJ .. (178:203)  
1:64 2. indicate to the applicants’.. (204:215)  
1:65 I must add in this context tha.. (219:219)  
1:66 Client was satisfied by Bytes .. (219:219)  
1:67 seized during the Anton Piller.. (222:222)  
1:68 Mr K. Yeo gave evidence in thi.. (222:222)  
1:69 Mr Yeo said “of late this cust.. (222:222)  
1:70 Defendant said in his affidavi.. (222:222)  
1:71 I may add at this stage, Defen.. (222:222)  
1:72 During cross-examination on th.. (222:222)  
1:73 It was First Plaintiff’s case .. (225:225)  
1:74 THE PARITALA E-MAILS: In this .. (228:229)  
1:75 He was provided with electroni.. (236:236)  
1:76 trace the e-mails and establis.. (237:237)  
1:77 I have already mentioned that .. (237:237)  
1:78 analysed the e-mails, extracte.. (238:238)  
1:79 The analysis involved expertis.. (238:238)  
1:80 which is fully reflected in th.. (238:238)  
1:81 From the e-mail which was rece.. (240:240)  
1:82 The same information was refle.. (242:242)  
1:83 The e-mail sent 4:28 on 3 Febr.. (245:245)  
1:84 All these documents reflect th.. (247:247)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:85 On 3 February 2010 at 4:33 ano.. (249:249)
- 1:86 The e-mails were originally se.. (254:254)
- 1:87 These annexures were not print.. (256:256)
- 1:88 They were also not forwarded t.. (258:258)
- 1:89 These annexures were printed t.. (260:260)
- 1:90 From the files' Meta-data it w.. (264:264)
- 1:91 Whether Defendant gave the doc.. (266:266)
- 1:92 The Applicants were also grant.. (269:269)
- 1:93 two computer hard drives and t.. (269:269)
- 1:94 Centurion Sheriff two computer.. (269:269)
- 1:95 forensically analyse the elect.. (269:269)
- 1:96 gave evidence as to what he di.. (269:269)
- 1:97 He had utilised keywords to lo.. (271:271)
- 1:98 Defendant's user name on his c.. (273:273)
- 1:99 He located references to all t.. (275:275)
- 1:100 He located the original e-mail.. (277:277)
- 1:101 He also stated that it was bey.. (279:279)
- 1:102 When searching for other commu.. (282:282)
- 1:103 Defendant was still in possess.. (287:287)
- 1:104 in the context of the data col.. (296:296)
- 1:105 The integrity of the data coll.. (296:296)
- 1:106 During March/April 2008 she wa.. (300:300)
- 1:107 He had worked for Bytes since .. (304:309)
- 1:108 On 23 April he sent an e-mail .. (310:314)
- 1:109 The new policy that he had sug.. (315:315)
- 1:110 as to fall in line the best pr.. (315:315)
- 1:111 After Defendant had made publi.. (318:318)
- 1:112 They found that no fraud had b.. (318:318)
- 1:113 Cross-examination of Mr Yeo: D.. (320:321)
- 1:114 Third Defendant testified that.. (324:324)
- 1:115 Second Plaintiff also testifie.. (324:324)
- 1:116 Ms Grune gave evidence about t.. (330:330)
- 1:117 For that purpose her mandate w.. (330:330)
- 1:118 The review was performed also .. (330:330)
- 1:119 Data records of incidents logg.. (337:337)
- 1:120 Policy documents and procedure.. (339:339)
- 1:121 They performed data analysis o.. (341:341)
- 1:122 KPMG's calculations were compa.. (343:343)
- 1:123 They documented findings and c.. (345:345)
- 1:124 They performed tests to verify.. (347:347)
- 1:125 KPMG recommends that a System .. (358:358)
- 1:126 Corrections should not be allo.. (358:358)
- 1:127 34. During cross-examination b.. (369:370)
- 1:128 According to the KPMG Report, .. (373:373)
- 1:129 I may just say at this stage t.. (376:376)
- 1:130 I may also mention briefly at .. (376:376)
- 1:131 Ms. le Hanie, the Second Plain.. (380:380)
- 1:132 She has deposed to five affida.. (380:381)
- 1:133 She mentioned that during June.. (384:384)
- 1:134 Ms le Hanie was in my view a l.. (387:387)
- 1:135 40. She remembers that probabl.. (389:390)
- 1:136 Ms le Hanie then gave evidence.. (393:393)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:137 Since the false allegations we.. (396:396)
- 1:138 The business of First Plaintiff.. (399:399)
- 1:139 DEFENDANT’S CROSS-EXAMINATION .. (402:402)
- 1:140 MR I VAN DER MERWE: (412:412)
- 1:141 DEFENDANT’S CROSS-EXAMINATION:... (428:428)
- 1:142 Every client had a different S.. (429:429)
- 1:143 DEFAMATION: APPLICABLE LEGAL P.. (441:441)
- 1:144 Khumalo and Others vs Holomisa.. (443:443)
- 1:145 Crawford vs Albu 1917 AD 102 a.. (455:455)
- 1:146 LAWSA, Volume 17 page 237. (457:457)
- 1:147 SA Associated Newspapers Ltd v.. (459:459)
- 1:148 Neethling vs Du Preez, Neethli.. (464:464)
- 1:149 Le Roux vs Dey 2010 (4) SA 210.. (466:466)
- 1:150 National Media Ltd vs Bogoshi .. (470:470)
- 1:151 : Delta Motor Corporation (Pty.. (472:472)
- 1:152 Crawford vs Albu supra (475:475)
- 1:153 Suid Afrikaanse Uitsaai Ko-ope.. (479:479)
- 1:154 Suid Afrikaanse Uitsaai Ko-ope.. (481:481)
- 1:155 The attachments to those e-mai.. (489:489)
- 1:156 IS CONTEMPT OF COURT ESTABLISH.. (505:505)
- 1:157 : Fakie N.O vs CC11 Systems (P.. (507:507)
- 1:158 Jayiya vs MEC for Welfare East.. (509:509)
- 1:159 Clement vs Clement 1961 (3) SA.. (510:510)
- 1:160 S vs Van der Meyden 1999 (1) S.. (512:512)
- 1:161 R vs De Villiers 1944 AD 493 a.. (514:514)
- 1:162 e: S vs Sauls and Others 1981 .. (516:516)
- 1:163 Court must consider the nature.. (525:530)
- 1:164 Media 24 Ltd and Others vs SA .. (553:553)
- 1:165 AA Alloy Foundry (Pty) Ltd vs .. (555:555)
- 1:166 Setlogelo vs Setlogelo 1914 AD.. (559:559)
- 1:167 Hix Networking Technologies vs.. (560:560)
- 1:168 Le Roux and Others vs Dey [201.. (562:562)

**Codes**

---

- Background {10-0}
- CE {3-0}
- CE1 {4-2}
- CE2 {9-2}
- CE3 {8-2}
- CE4 {9-4}
- CE5 {9-2}
- IE1 {5-3}
- IE2 {3-3}
- IE3 {4-1}
- IE4 {2-1}
- IE5 {6-1}
- IE6 {12-2}
- IE7 {13-1}
- IE8 {33-8}
- IE9 {2-1}

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

LE1 {3-3}  
LE2 {8-6}  
LE3 {4-10}  
LE4 {33-1}  
LE5 {3-1}  
Ruling - eEvidence Accepted. {1-0}

**Memos**

---

Alignment of Industry to Law - LE2: IE2 {0-0 Commentary} - Super

Comment:

Electronic evidence presented was obtained using forensically sound tools and methods, as prescribed by the Criminal Procedure Act.

CIRT Technical Duties IE1-8: LE3 {0-0 Commentary} - Super

Comment:

Law enforcement and independent computer forensic expert/s demonstrated to the courts that evidence obtained was done by following forensic standards and processes. The courts admitted all electronic evidence presented.

Demonstrate Procedural Compliance - CE3: LE2: IE8 {0-0 Commentary} - Super

Comment:

Employees testified on the existence of organisational policies and procedures, and how these were based on best practice and industry standards. The resulting evidence was admitted by the court.

Evidence Processing - CE4: IE2: LE3 {0-0 Commentary} - Super

Comment:

Bytes employees demonstrated competence and offered testimony proving that evidence was collected using forensically sound manner. Evidence obtained by law enforcement during the execution of an Anton Pillar and that obtained from Bytes was admitted by the court.

Evidentiary Value Preservation - CE5: IE1: LE2 {0-0 Commentary} - Super

Comment:

Bytes was able to demonstrate that their systems maintained data integrity, and presented system logs and email records which the court admitted. The items seized during Anton Pillar execution were also admitted as evidence in support of Bytes' argument.

Expert Witness Preparation CE4: LE2: IE8 {0-0 Commentary} - Super

Comment:

The witnesses demonstrated competence and due preparation for court proceedings. The courts concluded that Bytes' witnesses were credible.

Justice Duties LE5: IE3 {0-0 Commentary} - Super

Comment:

The justice system sought to have a fair trial, interpreted evidence presented and imposed fines against the defendant.

Policy Framework CE2: LE1: IE8 {0-0 Commentary} - Super

Comment:

Bytes demonstrated existence of forensic ready policies, and employees testified of how the defendant's fraud allegations were false, leading to the KPMG (system) audit. The audit showed that the system maintained data integrity and made improvement recommendations.

Prosecution of e-crimes - LE4: IE8 {0-0 Commentary} - Super

Comment:

Justice personnel extensively cross-examined electronic evidence presented, referred to

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

prior case law and sought assistance of external experts (KPMG) to verify findings.  
Standards Framework - CE1: IE8:LE1 {0-0 Commentary} - Super

Comment:

Employees at Bytes testified that Policies were developed in line with best practice and Industry Standards. Standards were in compliance with the law (Privacy Law/Competition Law).

### Network Views

---

Alignment of Industry to Law - LE2: IE2 (3)  
CIRT Technical Duties IE1-8: LE3 (11)  
Demonstrate Procedural Compliance - CE3: LE2: IE8 (4)  
Evidence Processing - CE4: IE2: LE3 (4)  
Evidentiary Value Preservation - CE5: IE1: LE2 (4)  
Expert Witness Preparation CE4: LE2: IE8 (4)  
Justice Duties LE5: IE3 (3)  
M-DiFoRe Network Links - Case 2 (19)  
Policy Framework CE2: LE1: IE8 (4)  
Prosecution of e-crimes - LE4: IE8 (3)  
Standards Framework - CE1: IE8:LE1 (4)

### Code-Links

---

CE1 <is property of> LE1  
CE2 <comply with> IE8  
CE2 <comply with> LE1  
CE3 <is property of> LE2  
CE4 <comply with> IE2  
CE4 <comply with> LE2  
CE4 <Cooperate with> LE3  
CE4 <must achieve> IE8  
CE5 <comply with> LE2  
CE5 <must achieve> IE1  
IE2 <comply with> LE2  
IE8 <comply with> CE1  
IE8 <comply with> CE3  
IE8 <comply with> LE1  
IE8 <comply with> LE2  
LE2 <is associated with> IE1  
LE3 <comply with> IE1  
LE3 <comply with> IE2  
LE3 <comply with> IE3  
LE3 <comply with> IE4  
LE3 <comply with> IE5  
LE3 <comply with> IE6  
LE3 <comply with> IE7  
LE3 <comply with> IE8  
LE3 <comply with> IE9  
LE4 <comply with> IE8  
LE5 <is associated with> IE6

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

## Appendix 7: Case Study 3: Atlas.ti Coding Summary Report

---

List of all objects

---

HU

---

POST BANK CASE\_CH6

**Primary Doc**

---

P 1: POST BANK CASE REPORT.rtf {110}

**Quotations**

---

1:1 Respondent (31:31)  
1:2 The applicants have instituted.. (38:38)  
1:3 arrested (41:41)  
1:4 applicants were charged with c.. (41:41)  
1:5 section 2(1)(e)(f) read with s.. (41:41)  
1:6 racketeering activity, money l.. (41:41)  
1:7 section 49 G (3) of The Act. (44:44)  
1:8 trial which commenced on 27 Ja.. (44:44)  
1:9 (4) Section 49G (1) of The Act.. (47:47)  
1:10 (i)section 49G (3) provides: ‘.. (48:48)  
1:11 (5)In terms of article 2(b), J.. (50:50)  
1:12 (i)article 6(2) provides: “In .. (51:51)  
1:13 (4) Section 49G (1) of The Act.. (47:48)  
1:14 (6)The charges preferred again.. (54:54)  
1:15 RESPONDENT’S (56:56)  
1:16 Captain Jacobus Hansen, the in.. (57:57)  
1:17 respondent’s opposition to the.. (57:57)  
1:18 application (38:38)  
1:19 (2) The first to the seventh a.. (41:41)  
1:20 Subsequent to their arrest the.. (41:41)  
1:21 (3) Subsequent to their arraig.. (43:43)  
1:22 On 26 August 2013, the first t.. (44:44)  
1:23 THE LEGAL FRAME WORK (46:46)  
1:24 (ii)article 8(1) regarding the.. (52:52)  
1:25 THE RESPONDENT’S PRIMA FACIE C.. (56:56)  
1:26 affidavit (57:57)  
1:27 except the fourth and sixth ap.. (57:57)  
1:28 made submissions through their.. (57:57)  
1:29 affidavit (59:59)  
1:30 The applicants were arrested a.. (59:59)  
1:31 (9)The details of some of the .. (61:61)  
1:32 The discovery of the various b.. (63:63)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:33 The details relating to these .. (63:63)
- 1:34 After his arrest, the first ap.. (63:63)
- 1:35 The first applicant has allege.. (65:65)
- 1:36 evidence (67:67)
- 1:37 The rest of the applicants hav.. (67:67)
- 1:38 The applicants are charged wit.. (68:68)
- 1:39 documentary evidence (68:68)
- 1:40 Post Office branches where the.. (68:68)
- 1:41 found on the second to ninth a.. (68:68)
- 1:42 Cell phone communications betw.. (70:70)
- 1:43 (14) Cell phone communications.. (70:70)
- 1:44 Cell phone communications (70:70)
- 1:45 The respondent intends to lead.. (72:72)
- 1:46 If one of the applicants shoul.. (72:72)
- 1:47 Counsel argued that the first .. (75:75)
- 1:48 He will not conceal or destroy.. (77:77)
- 1:49 The trial has now commenced, c.. (80:80)
- 1:50 He joined in the initial secti.. (80:80)
- 1:51 interpretation (83:83)
- 1:52 Further counsel elected not to.. (84:84)
- 1:53 (19) Counsel elected to addres.. (83:83)
- 1:54 unsuccessfully launched a bail.. (87:87)
- 1:55 unsuccessfully launched a bail.. (87:87)
- 1:56 and is set down for the entire.. (89:89)
- 1:57 trial (89:89)
- 1:58 In her capacity as the acting .. (89:89)
- 1:59 (22) Her release will not enda.. (91:91)
- 1:60 (23) She is a single parent. H.. (93:93)
- 1:61 unsuccessful bail application... (99:99)
- 1:62 (25) Although the trial has co.. (101:101)
- 1:63 (26) The prolonged trial is ex.. (103:103)
- 1:64 She will not influence or inti.. (103:103)
- 1:65 If released she can afford to .. (108:108)
- 1:66 Organized Crime Act, (110:110)
- 1:67 cell phone records (110:110)
- 1:68 prof that they communicated wi.. (110:110)
- 1:69 she only executed three transa.. (110:110)
- 1:70 documentary evidence linking (112:112)
- 1:71 scope of her duties as a telle.. (112:112)
- 1:72 cell phone records show (112:112)
- 1:73 incriminating evidence found o.. (118:118)
- 1:74 linking (118:118)
- 1:75 He launched an unsuccessful ba.. (120:120)
- 1:76 There is no legal justificatio.. (120:120)
- 1:77 section 35 of The Constitution.. (123:123)
- 1:78 Counsel further submitted that.. (124:124)
- 1:79 (34) The enactment of section .. (126:126)
- 1:80 (35) The purpose of section 49.. (128:128)
- 1:81 (36) Pursuant to section 35(1).. (130:132)
- 1:82 (37) The continued further det.. (134:134)
- 1:83 It follows that although secti.. (136:138)
- 1:84 section 49 G (3) of The Act, (141:141)



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:85 (39) The charges against the a.. (142:142)  
1:86 (40) In considering the releas.. (144:144)  
1:87 (41) Because of the inquisitor.. (146:146)  
1:88 (42) Because the applicants ar.. (148:148)  
1:89 (43) The court is obliged to i.. (150:150)  
1:90 led evidence (152:152)  
1:91 cogent and credible and has th.. (152:152)  
1:92 The applicants have all made a.. (152:152)  
1:93 Post Office banking (152:152)  
1:94 cellular telephone records (154:154)  
1:95 establishing that the applican.. (154:154)  
1:96 cellular telephone records app.. (154:154)  
1:97 inference (154:154)  
1:98 cellphones (154:154)  
1:99 cellular (154:154)  
1:100 the inference may be drawn tha.. (154:154)  
1:101 affidavit. (156:156)  
1:102 Having regard to the strength .. (157:157)  
1:103 (47) A court in considering th.. (159:159)  
1:104 (48) The factual status quo ma.. (160:161)  
1:105 strength of the respondent's c.. (142:142)  
1:106 In considering the release or .. (144:144)  
1:107 (40) In considering the releas.. (144:144)  
1:108 evidence is cogent and credibl.. (152:152)  
1:109 possibility of establishing an.. (152:152)  
1:110 In considering whether the rel.. (163:171)

**Codes**

---

(2) The first to the seventh a.. {1-0}  
(5)In terms of article 2(b), J.. {1-0}  
(i)section 49G (3) provides: '.. {1-0}  
applicable law/elaw {13-0}

Arrest/verdict {1-0}

CE {4-0}~

Comment:

Postbank fraud case involving access to bank acc, data etc. use of cell phone evidence  
key in identifying fraudsters. state accepted tech used by postbank to have preserved call  
data etc. strong case.

CE1 {1-2}

CE2 {1-2}

CE3 {1-2}

CE4 {5-4}~

Comment:

accused were employees of Post Office

CE5 {8-2}

charges {1-0}

electronic data compromised {1-0}

IE1 {4-3}

IE1-9 {3-0}~

Comment:

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

eData compromised and uncovered during investigation. Accepted evidence by court  
IE2 {1-3}  
IE3 {4-1}  
IE4 {3-1}  
IE5 {6-1}  
IE6 {17-2}  
IE7 {1-1}  
IE8 {9-8}  
IE9 {3-1}  
intro {1-0}~  
Comment:

accused in correctional facility. evidence upheld.

L2 {1-0}  
LE {1-0}  
LE1 {7-3}  
LE2 {14-6}  
LE3 {8-10}~  
Comment:

arrested, state linked to prior matter.  
tried to escape.

LE4 {2-1}  
LE5 {11-1}~  
Comment:

able to link suspects to prior frauds.

LE6 {0-0}  
Modus operandi {1-0}  
section 49 G (3) of The Act. {1-0}  
trial {1-0}  
verdict {3-0}~  
Comment:

no evidence against her/employee

### Network Views

---

CE4-IE2 (2)  
CE5-LE2 (2)  
CE5-LE2-IE1 (3)  
IE2-LE2 (2)  
IE8-CE4 (2)  
LE2-CE4 (5)  
LE2-IE1 (2)  
LE3-CE4 (2)  
LE3 - others (17)  
LE5-IE6 (2)

### Code-Links

---

CE1 <is property of> LE1  
CE2 <comply with> IE8  
CE2 <comply with> LE1  
CE3 <is property of> LE2

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

CE4 <comply with> IE2  
CE4 <comply with> LE2  
CE4 <Cooperate with> LE3  
CE4 <must achieve> IE8  
CE5 <comply with> LE2  
CE5 <is cause of> IE1  
IE2 <comply with> LE2  
IE8 <comply with> CE1  
IE8 <comply with> CE3  
IE8 <comply with> LE1  
IE8 <comply with> LE2  
LE2 <is associated with> IE1  
LE3 <comply with> IE1  
LE3 <comply with> IE2  
LE3 <comply with> IE3  
LE3 <comply with> IE4  
LE3 <comply with> IE5  
LE3 <comply with> IE6  
LE3 <comply with> IE7  
LE3 <comply with> IE8  
LE3 <comply with> IE9  
LE4 <comply with> IE8  
LE5 <is associated with> IE6

## Appendix 8: Case Study 4: Atlas.ti Coding Summary Report

---

List of all objects

---

**HU**

---

Rejected case - Anton Piller on IP theft

**Primary Doc**

---

P 1: FRIEDSHELF 1509\_Main.rtf {81}

**Quotations**

---

1:1 C Whitcutt SC (with S Ebrahim).. (12:12)  
1:2 G Kairinos SC (with B Stevens (12:12)  
1:3 Applicants (21:21)  
1:4 respondent's (21:21)  
1:5 order (21:21)  
1:6 search (21:21)  
1:7 seizure (21:21)  
1:8 preservation (21:21)  
1:9 defamation and unlawful compet.. (21:21)  
1:10 Applicants alleged that respon.. (21:21)  
1:11 order allowing for the search .. (21:21)  
1:12 C Whitcutt SC (with S Ebrahim).. (40:41)  
1:13 search, seizure and preservati.. (42:42)  
1:14 Order . (a) The extended rule.. (43:49)  
1:15 This is the extended return da.. (53:53)  
1:16 The order permitted the applic.. (53:53)  
1:17 'Originals or copies of any em.. (54:55)  
1:18 supervising attorneys (56:56)  
1:19 forensic experts (56:56)  
1:20 to search and examine all elec.. (56:56)  
1:21 The order granted is in line w.. (57:57)  
1:22 Clause 3.3 of the order permit.. (57:57)  
1:23 [4] Pursuant to the order, the.. (61:61)  
1:24 [5] Unlike the order appearing.. (65:72)  
1:25 range of warehousing and distr.. (76:76)  
1:26 sophisticated software (76:76)  
1:27 first applicant's management t.. (76:76)  
1:28 [9] The respondent was employe.. (77:77)  
1:29 The respondent was employed by.. (77:77)  
1:30 It is I common cause that duri.. (77:77)  
1:31 It is I common cause that duri.. (77:80)  
1:32 restraint of trade agreement, (81:81)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

- 1:33 C (a) The respondent resigned .. (83:83)
- 1:34 (b) the respondent breached hi.. (84:84)
- 1:35 [13] On 19 July 2014 an anonym.. (89:89)
- 1:36 The applicants attribute the e.. (90:91)
- 1:37 The applicants had no direct e.. (92:92)
- 1:38 [17] The applicants allege tha.. (95:101)
- 1:39 simultaneously (103:103)
- 1:40 According to the report of the.. (104:104)
- 1:41 she surrendered he (104:104)
- 1:42 The order does not permit the .. (105:105)
- 1:43 The order does not permit the .. (105:105)
- 1:44 sheriff (105:105)
- 1:45 The sheriff should have refuse.. (105:111)
- 1:46 It also appears that 12 docume.. (115:116)
- 1:47 It also appears that 12 docume.. (115:115)
- 1:48 The inventory compiled by the .. (116:116)
- 1:49 The inventory compiled by the .. (116:116)
- 1:50 evidence was C obtained and se.. (116:116)
- 1:51 copying of the cellphone driv (117:117)
- 1:52 affidavit (117:117)
- 1:53 It does not appear from the af.. (117:117)
- 1:54 supervising attorney (117:117)
- 1:55 The inventory of items seized .. (118:118)
- 1:56 [32] Whilst the respondent ini.. (120:121)
- 1:57 No prima facie case was made o.. (126:126)
- 1:58 (a) No prima facie case was ma.. (126:126)
- 1:59 The applicants failed to make .. (131:131)
- 1:60 Anton Piller relief is not app.. (133:133)
- 1:61 ) The restraint of trade cove.. (135:135)
- ~1:62 [37] Certain of the respondent.. (138:140)

Comment:

justice correctly applying the law and interpreted facts.

- 1:63 irregularities in the executio.. (143:144)
- 1:64 What is of concern is the fact.. (145:145)
- 1:65 C [42] What is of concern is t.. (145:149)
- ~1:66 [49] An Anton Piller search-an.. (158:169)

Comment:

Specific process on application of Anton Pillers...this was not executed correctly.

Scope issues rendering evidence inadmissible. imaged wrong data, not that belonging to suspect as per order.

- 1:67 Both sets of counsel are agree.. (172:198)
- 1:68 The applicants failed to discl.. (206:206)
- 1:69 The applicants failed to discl.. (206:206)
- 1:70 While the applicants put up a .. (207:207)
- 1:71 The respondent has stated that.. (208:208)
- 1:72 The applicants' counsel in rep.. (211:211)
- 1:73 As there is no evidence linkin.. (216:216)
- 1:74 As there is no evidence linkin.. (216:216)
- 1:75 In the draft order the applica.. (220:220)
- 1:76 A difficulty which arises in t.. (221:221)
- 1:77 '[9.1] What the Practice Manua.. (225:235)
- 1:78 In my view the practice needs .. (236:236)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

1:79 In my view the practice needs .. (236:239)  
1:80 Documents and information are .. (116:116)  
1:81 restore (46:46)

**Codes**

---

Analysis (IE5) {1-1}~

Comment:

Analysis of evidence and its attributes.

failed to find evidence linking suspect to email in question.

Applicant {1-0}

Case of defamation & interference with contract obligations {1-0}

CE {1-0}

Charge {1-0}

CO {1-0}

Collection (IE2) {2-3}~

Comment:

Correct method/tools to collect evidence without compromising forensic integrity.

Technical experts used correct tools but not correct process, thereby compromising forensic integrity.

imaged but imaged the wrong items.

imaged before checking for existence of relevant data, thus going against court order.

Criminal Process (LE2) {13-6}~

Comment:

Correct application of the Criminal Process in ensuring evidence discovery, maintaining integrity of evidence seized, and adherence to due process

Failed to operate within scope set by court order.

Failed to operate within scope by taking wife's tablet, phone etc.

Failed to identify key items to be imaged, failed to follow correct process in imaging (did not review relevance of content before imaging, as per Anton Piller order)

DFR Technologies (CE5) {2-2}~

Comment:

Digital Forensic Ready technology to maintain forensic attributes in all data stored.

Organisation demonstrated existed of industry forensic ready technology

Documentation (IE7) {4-1}~

Comment:

Thorough documentation and chain of custody relating to the case.

Sherriff and CF Expert failed to keep detailed inventory re contents of drive etc.

Sup attorney failed to review and correct.

Electronic Laws (LE1) {3-3}~

Comment:

Comprehensive legislation detailing compliance specifications

Anton Pillar order was issued in line with electronic laws, in favor of the organisation.

email in question {1-0}

Human Resources (CE4) {7-4}~

Comment:

Ability to operate forensic ready technology, and provide expert witness.

## DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR EVIDENTIARY DATA HANDLING

RTT representatives failed to disclose key info during testimony.  
Identification (IE4) {1-1}~

Comment:

Identification of key evidence attributes for analysis.

Failed to identify key attributes to ensure compliance with court order.

didn't look at identities registry to confirm user of devices. resulting in items out of scope being included/imaged.

IE1-7 {4-0}~

Comment:

failed to identify key items to be imaged, failed to follow correct process in imaging (did not review relevance of content before imaging, as per Anton Piller order)

IE1-8 {2-0}~

Comment:

failure to apply digital forensic investigation process to correctly identify correct sources of evidence, preserve, analyze and validate on data sources to correctly place suspect behind the computer and prove all identities.

failure to hypothesize during analysis and interpretation to ensure all findings are tested.

Interpretation (IE6) {1-2}~

Comment:

Correct interpretation of findings during investigation and analysis stage.

CIRT failed to find evidence linking suspect to email in question. not all logs and pertinent data (IP address, email headers, etc.) was verified to link suspect to email.

Justice Personnel (LE5) {11-1}~

Comment:

Correct interpretation of digital forensic results during prosecution stage.

magistrate correctly applied the law and identified all the tech flaws in the case and made valid recommendations to improve the process.

lack of full disclosure re relationship to suspect impacted case negatively.

Justice System (LE3) {2-10}~

Comment:

Ability to interpret and prosecute cases involving electronic evidence.

Supervising attorneys demonstrated a lack of E.T.C in the overseeing the correct processing of electronic evidence.

scope of order was not complied to as items outside scope were imaged etc.

correct process was not followed in identifying items to be seized and imaged etc

Law Enforcement Agents (LE4) {5-1}~

Comment:

Knowledge and willingness to investigate e-crimes.

Error not with police but sup attorney and staff

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Supervising attorney failed to ensure electronic evidence is processed as per the court order

Supervising attorney role was to ensure law is upheld.

Policies (CE2) {4-2}~

Comment:

Organisation to develop policies that govern forensic readiness.

Organisation demonstrated existence of industry policies, technology and ETC of staff.

Presentation (IE8) {6-8}~

Comment:

Demonstration/Application of education, training and certification of CIRT/Witnesses on presentation of evidence.

Witnesses/respondents failed to disclose all relevant facts, resulting in charges being dropped.

Respondent denied charges. strong testimony.

Applicant failed to disclose that respondent was employed at RTT prior to case. affects judgment on nature of relationship and how respondent received access to email list.

RTT representatives failed to present a strong case. too many mistakes on scope and application of order.

Preservation (IE1) {4-3}~

Comment:

Evidence preserved in accordance with industry standards and aligned to legislative requirements.

Evidence preserved (some) was outside the scope of the court order, and was not done following correct procedure.

Procedures (CE3) {7-2}~

Comment:

Organisation to develop procedures that govern forensic readiness.

Organisation demonstrated existence of procedures

applicant and responded agreed to cooperate

Respondent {1-0}

Retention (IE9) {1-1}~

Comment:

Retention of evidence as required by law.

court ordered to restore what was retained.

Standards (CE1) {2-2}~

Comment:

Organisational standards developed in harmony with legislative requirements.

Organisation demonstrated existence of industry standards

Summary of case {1-0}



**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

Validation (IE3) {1-1}~

Comment:

Validating evidence for relevance and corroboration.

Failed to validate evidence for reliance

### **Network Views**

---

Evidence Collection IE2 | LE2 (2)  
Evidence Handling CE4 | LE3 | IE2 (3)  
Evidence Preservation CE5 | IE1 | LE2 (3)  
Justice System Implementation LE5 | IE6 (2)  
M-DiFoRe Network Links (19)  
Methodology Evaluation LE3 - IE1 to IE9 (10)  
Policy Alignment CE2 | IE8 | LE1 (3)  
Procedural Implementation IE8 | CE3 | LE2 (3)  
Prosecution of e-crimes LE4 IE8 (2)  
Standards Localisation IE8 | CE1 | LE1 (3)  
Witness Preparation CE4 | IE8 | LE2 (3)

### **Code-Links**

---

Collection (IE2) <comply with> Criminal Process (LE2)  
Criminal Process (LE2) <is associated with> Preservation (IE1)  
DFR Technologies (CE5) <comply with> Criminal Process (LE2)  
DFR Technologies (CE5) <is cause of> Preservation (IE1)  
Human Resources (CE4) <comply with> Collection (IE2)  
Human Resources (CE4) <comply with> Criminal Process (LE2)  
Human Resources (CE4) <Cooperate with> Justice System (LE3)  
Human Resources (CE4) <must achieve> Presentation (IE8)  
Justice Personnel (LE5) <is associated with> Interpretation (IE6)  
Justice System (LE3) <comply with> Analysis (IE5)  
Justice System (LE3) <comply with> Collection (IE2)  
Justice System (LE3) <comply with> Documentation (IE7)  
Justice System (LE3) <comply with> Identification (IE4)  
Justice System (LE3) <comply with> Interpretation (IE6)  
Justice System (LE3) <comply with> Presentation (IE8)  
Justice System (LE3) <comply with> Preservation (IE1)  
Justice System (LE3) <comply with> Retention (IE9)  
Justice System (LE3) <comply with> Validation (IE3)  
Law Enforcement Agents (LE4) <comply with> Presentation (IE8)  
Policies (CE2) <comply with> Electronic Laws (LE1)  
Policies (CE2) <comply with> Presentation (IE8)  
Presentation (IE8) <comply with> Criminal Process (LE2)  
Presentation (IE8) <comply with> Electronic Laws (LE1)  
Presentation (IE8) <comply with> Procedures (CE3)  
Presentation (IE8) <comply with> Standards (CE1)  
Procedures (CE3) <is property of> Criminal Process (LE2)  
Standards (CE1) <is property of> Electronic Laws (LE1)

**DEVELOPING A MULTIDISCIPLINARY DIGITAL FORENSIC READINESS MODEL FOR  
EVIDENTIARY DATA HANDLING**

**Appendix 9: Completed Self-Assessment**

---

(1) M-DiFoRe Systems	Component Existence (Step 1)					System Existence (Step 2)					System Interdependencies (Step 3)					Remediation (Step 4)				
	(2) Component Name	(3) Exist (Y/N)	(4) Supporting Evidence Type & Source				(5) Exist (Y/N)	(6) Supporting Evidence Type & Source				(7) Nature of dependency			(8) Model Compliance (N,P,F)	(9) Supporting Evidence Type & Source				(10) Model Reference
			D	P	S	A		D	P	S	A	(7.1) Links	(7.2) Link Type (Co, Coo, Pr, Ac, As)	(7.3) Arrow Type (Uni-D, Bi-D)		D	P	S	A	
Evidence Collection (IE2, LE2)	IE2: Collection	Y	1, 4			1, 23-25	Y	1, 4, 6, 21			1, 23-25	L2, IE2	Co	Uni-D	F	1, 4, 6, 21			1, 23-25	6.3.3.1(i)
	LE2: Criminal Process	Y	1, 6, 21																	
Justice System Implementation (LE5, IE6)	LE5: Justice Personnel	Y	2				Y	1, 2		11, 12	1	LE5, IE6	As	Bi-D	F	1, 2		11, 12	1	6.3.3.1(ii)
	IE6: Interpretation	Y	1		11, 12	1														
e-Crime Prosecution (LE4, IE8)	LE4: Law Enforcement	Y	2				Y	1, 2, 30		11, 12, 15-20, 33-36	1	LE4, IE8	Co	Uni-D	F	1, 2, 30		11, 12, 15-20, 33-36	1	6.3.3.1(iii)
	IE8: Presentation	Y	1, 30			1														
Evidence Handling (CE4, LE3, IE2)	CE4: Human Resources	Y	8, 9				Y	1, 2, 4, 5, 7-9, 26		32	1, 23-25	CE4, LE3	Coo	Uni-D	F	1, 2, 5, 7, 8, 9, 26		32		6.3.3.2(i). Strict adherence to court order on evidence to be collected.
	LE3: Justice System	Y	1, 2, 5, 7, 26		32	CE4, IE2						Co	Uni-D	P	1, 4, 8, 9		1, 23-25			
	IE2: Collection	Y	1, 4			1, 23 - 25						LE3, IE2	Co	Uni-D	F	1, 2, 4, 5, 7, 26		32	1, 23-25	
Standards Localisation (IE8, CE1, LE1)	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1	Y	1, 3, 22, 30		11, 12, 15-20, 33-36	1	IE8, CE1	Co	Uni-D	F	1, 30		11, 12, 15-20, 33-36	1	6.3.3.2(ii). Present evidence that is within scope of court order. Full disclosure of facts.
	CE1: Standards	Y	1			CE1, LE1						Pr	Uni-D	F	1, 3, 22					
	LE1: Electronic Laws	Y	1, 3, 22									IE8, LE1	Co	Uni-D	P	1, 3, 22, 30		11, 12, 15-20, 33-36		
Policy Alignment (CE2, IE8, LE1)	CE2: Policies	Y	1, 10				Y	1, 3, 10, 22, 30		11, 12, 15-20, 33-36	1	CE2, IE8	Co	Uni-D	F	1, 10, 30		11, 12, 15-20, 33-36	1	6.3.3.2(iii). Present evidence that is within scope of court order. Full disclosure of facts.
	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1						IE8, LE1	Co	Uni-D	P	1, 3, 22, 30		11, 12, 15-20, 33-36		
	LE1: Electronic Laws	Y	1, 3, 22									CE2, LE1	Co	Uni-D	F	1, 3, 10, 22				
Witness Preparation (CE4, IE8, LE2)	CE4: Human Resources	Y	8, 9				Y	1, 6, 8-9, 21, 30		11, 12, 15-20, 33-36	1	CE4, LE2	Co	Uni-D	P	1, 6, 8, 9, 21				6.3.3.2(iv). Employees to present all facts to the court. Testimony given to court to be based on evidence within scope of court order. Criminal process to be fully complied with.
	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1						CE4, IE8	Ac	Uni-D	P	1, 8, 9, 30		11, 12, 15-20, 33-36		
	LE2: Criminal Process	Y	1, 6, 21									IE8, LE2	Co	Uni-D	P	1, 6, 21, 30		11, 12, 15-20, 33-36		
Procedural Implementation (IE8, CE3, LE2)	IE8: Presentation	Y	1, 30		11, 12, 15-20, 33-36	1	Y	1, 6, 10, 21, 30		11, 12, 15-20, 33-36	1	IE8, CE3	Co	Uni-D	P	1, 10, 30		11, 12, 15-20, 33-36	1	6.3.3.2(v). Testimony to demonstrate compliance with organisational procedures and the criminal process.
	CE3: Procedures	Y	1, 10			IE8, LE2						Co	Uni-D	P	1, 6, 21, 30		11, 12, 15-20, 33-36			
	LE2: Criminal Process	Y	1, 6, 21									CE3, LE2	Pr	Uni-D	F	1, 6, 10, 21				
Evidence Preservation (IE8, CE3, LE2)	CE5: DFR Technologies	Y				9, 15	Y	1, 4, 6, 21, 27, 28	14	1, 9, 15, 23-25		CE5, IE1	Ac	Uni-D	N	1, 4	27, 28	14	1, 9, 15, 23-25	6.3.3.2(vi). Correct implementation and configuration of DFR technologies, including event logging.
	IE1: Preservation	Y	1, 4	27, 28	14	1, 23-25						LE2, IE1	As	Bi-D	F	1, 6, 4, 21	27, 28	14	1, 23-25	
	LE2: Criminal Process	Y	1, 6, 21									CE5, LE2	Co	Uni-D	F	1, 6, 21			9, 15	
Methodology Evaluation (LE3, IE1-IE9)	LE3: Justice System	Y	1, 2, 5, 7, 26		32		Y	1, 2, 4, 5, 22, 26, 30, 31	27-29	11, 12, 14-20, 32-36	1, 23-25	-	-	-	-	-	-	-	6.3.3.3. Application of digital forensic process on evidence that falls within scope of court order. Correct documentation of process followed, especially inventory lists. Forensic methodology to be applied correctly.	
	IE1: Preservation	Y	1, 4	27, 28	14	1, 23-25						LE3, IE1	Co	Uni-D	P	1, 2, 4, 5, 7, 26	27, 28	14, 32		1, 23-25
	IE2: Collection	Y	1, 4			1, 23-25						LE3, IE2	Co	Uni-D	F	1, 2, 4, 5, 7, 26		32		1, 23-25
	IE3: Validation	Y	1			1						LE3, IE3	Co	Uni-D	P	1, 2, 5, 7, 26		32		1
	IE4: Identification	Y	1			1						LE3, IE4	Co	Uni-D	P	1, 2, 5, 7, 26		32		1
	IE5: Analysis	Y	1			1						LE3, IE5	Co	Uni-D	P	1, 2, 5, 7, 26		32		1
	IE6: Interpretation	Y	1		11, 12	1						LE3, IE6	Co	Uni-D	P	1, 2, 5, 7, 26		11, 12, 32		1
	IE7: Documentation	Y	1, 31	29		1						LE3, IE7	Co	Uni-D	P	1, 2, 5, 7, 26, 31	29	32		1
	IE8: Presentation	Y	1, 30			1						LE3, IE8	Co	Uni-D	P	1, 2, 5, 7, 26, 30		11, 12, 15-20, 32-36		1
	IE9: Retention	Y	1, 22			1						LE3, IE9	Co	Uni-D	F	1, 2, 5, 7, 22, 26		32		1