A Model for Digital Evidence Admissibility Assessment

by

Albert Antwi-Boasiako

A thesis submitted in fulfilment of the requirements for the degree

Doctor of Philosophy

in

Computer Science

in the

Faculty of Engineering, Built Environment and Information Technology

at the

University of Pretoria

Academic Supervisor: Professor Hein S. Venter

September 2018

ABSTRACT

Riding on the tide of the current development in computing and internet technologies, criminals have transitioned to the use of computer systems and digital channels to commit crimes. This transformation of crime requires criminal justice actors to investigate, produce and present digital evidence through a process that is scientifically proven and legally admissible, but also capable of securing successful prosecutions.

Even though previous efforts by criminal justice practitioners and researchers have contributed to the standardisation of digital forensics in a manner that has consolidated the *scientificity*[1] of digital forensics as a forensic science, these approaches, processes and techniques have not addressed adequately the issue of admissibility of digital evidence in judicial proceedings. In other words, existing models and standards are generally investigative-focused, which has significantly ensured that digital forensics processes follow a specific scientific order. Despite these advances, the existing *techno-legal dilemma* pertaining to the admissibility of digital evidence in judicial proceedings remains unresolved.

In order to address this *techno-legal dilemma*, the thesis presents a Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA), a model that integrates both technical and legal determinants to establish digital evidence admissibility in judicial proceedings. In order to operationalise the HM-DEAA, this research introduces an algorithm to assess digital evidence admissibility and to determine the evidential weight of a piece of digital evidence, which is tendered in a court of law. This algorithm has been tested on both hypothetical and real cases as part of the HM-DEAA's evaluation for its

[1] Words in italics are terminologies, which the researcher has introduced into the thesis. Definition of these terminologies are provided in Appendix B

potential use in legal proceedings. In addition, an expert system has been introduced to automate the operationalization of the HM-DEAA.

In practice, the HM-DEAA framework is expected to provide a harmonised techno-legal foundation for assessing digital evidence admissibility in the criminal justice sector. The model is expected to be used primarily by judges as a judicial tool in legal proceedings. The expert system is also expected to serve as an assessment tool for investigators, prosecutors and defence lawyers to evaluate digital evidence with regard to its potential use in court.

ACKNOWLEDGEMENTS

The development of the thesis has been one of the most important milestones of my intellectual and professional development journey. I must confess that; the journey has been a gratifying experience.

From my own philosophical perspective, this thesis represents my modest contribution to the development of humankind. I have always been amazed about the *human condition* and humanity's continuous strides to improve upon this *human condition.* The application of science and law for the purpose of justice is undeniably one of the most important demonstrations of humankind's efforts to address its existential fragilities and I am humbled to have contributed to this noble cause through this research.

This journey would have been impossible without the support and guidance of many who share the vision and the will to contribute to improving the *human condition*. I am thankful to God for my very existence and my peculiar state of mind, which has contributed to this research. I am grateful to the following people who have either impacted my thinking or supported me with this research:

- My deceased father, whose thinking, guidance and the values he instilled in us have permanently impacted my intellectual development and my understanding of the *human condition.*

- My family, especially my mother, Janet, my wife, Dorcas, my daughter, Michelle and my niece, Judith for their prayers, encouragement, patience and support for my intellectual pursuits.

- My academic supervisor, Professor Hein S. Venter for his scholarly guidance and professional support during the period of this research.

- Professional colleagues and staff of the e-Crime Bureau, especially Justice Afia S. Asare-Botwe, Dr Edgar F. A. Cooke, Sir Samuel Aning, Sir Philemon Hini, Ms. Elizabeth Mante, Ms. Matilda Anku, Sir Matthew Yankey Jnr. Sir Reindolf Boadu and Sir Mutaru Mumuni Muqthar for their excellent support with research for and review of the thesis.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

PART 1: INTRODUCTION

Part One of the thesis introduces the research work at hand. This part consists only of the introduction chapter. The introduction chapter discusses the motivation for the study and introduces the research problem. It discusses the key research questions framing this study. Research methodology, terminologies used in the research and the organisation of the thesis are also addressed in this chapter.

CHAPTER 1: INTRODUCTION

1.1. Introduction

The domain of digital forensics is as new to academia as it to courts of law across many jurisdictions around the world. Despite the emerging significance of digital evidence in the delivery of justice in our current information technology-driven world, digital forensics as a forensic science is still undergoing transformation. This transformation is underpinned by the evolving dynamics in the information technology sector and the development and evolution of cybercrimes and legal responses to criminality arising from information technology advancement. The cyberspace has become a conduit for almost every crime from theft of personal data to child pornography [1]. According to Interpol, many traditional crimes have assumed new dimensions with the advent of the internet and digital tools [2].

The application of digital forensics in the criminal justice sector is significant. Digital forensics is not only applied in cyber-dependent incidents, its application has also been momentous in cyber-facilitated crimes. This is due to the fact that in practice, it is nearly impossible in today's information technology-driven society to find a crime without any digital dimension [3]. Cyber-dependent crimes are crimes that can only be committed using a computer, networks or any other information technology infrastructure or digital device. Examples of such crimes include hacking and denial of service attacks. Cyber-facilitated crimes, on the other hand, are conventional crimes that are perpetrated using computers, network technologies or any other information technology infrastructure or digital device. Examples of such cases include human trafficking, terrorism and economic crimes such as financial fraud and money laundering.

Historically, the significant impact of information technology on crime necessitated the birth and development of digital forensics. Consequently, the importance of digital evidence, especially in the criminal justice sector cannot be ignored. As a result of this inter-relationship, several efforts have been made by law enforcement agencies, professional associations, academia and scientific communities to organise digital forensics into a formal scientific discipline. For example, the first Digital Forensic Research Workshop (DFRWS) proposed a standardised framework for digital forensics [4]. Reith et. al. [5] proposed a digital forensics process model, which is normally referred to as the *'abstract model'.* Valjarevic and Venter [6] have proposed a harmonised digital forensics model aimed at resolving the various fragmentations associated with digital forensics processes. The Association of Chief Police Officers' (ACPO) Good Practice Guide [7] and the U.S. Department of Justice (DOJ) Electronic Crime Scene Investigation Guide [8] are examples of efforts made within law enforcement circles to harmonise digital forensics processes and activities.

Standardisation of digital forensics achieved a major milestone when the International Organisation for Standardization (ISO) published standard ISO/IEC 27037 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence in 2012 [9] and standard ISO/IEC 27043 — Incident Investigation Principles and Processes in 2015 [10]. Both standards provide guidelines that encapsulate different digital forensics processes and models into a harmonised investigations framework for various incident investigations.

Despite the significant developments in rationalizing digital forensics, existing standards and models do not adequately address the issue of digital evidence admissibility in judicial proceedings. This is because the question of digital evidence admissibility hinges on a *techno-legal dilemma* — the difficulty of establishing a balanced but also interdependent relationship between the various technical and the legal determinants for the purposes of establishing a harmonised scientific foundation to aid the admissibility of digital evidence in judicial proceedings. As a result, any scholarly effort aimed at addressing this question should take into consideration this foundational problem of digital evidence admissibility in judicial processes. The term *techno-legal dilemma* is explained further in the problem statement section of the thesis.

The researcher has identified the need for a framework that harmonises both technical and legal determinants to provide a foundation for the admissibility of digital evidence. It is also important to emphasize that the transnational nature of computer crimes and emerging international cooperation frameworks require an integrated response through a harmonised techno-legal framework to ensure *digital evidence interoperability* across different jurisdictions.

The remainder of the introductory chapter is organised as follows: Section 1.2 focuses on the motivation for the research whilst section 1.3 introduces the problem statement and research questions arising from the research theme. Section 1.4 discusses the research methodology and design with section 1.5 focusing on key terminologies associated with the research. Section 1.6 discusses the layout of the thesis. Section 1.7 ends this chapter with a brief conclusion.

1.2. Motivation for the Study

Despite recent advances, digital forensics is a relatively new domain of research. Research interest in this discipline has expanded in the last few years, with diverse experts looking into the various and often complex dimensions of the application of forensic science in the ever-evolving information technology environment.

According to a research article published on the Forbes website, cybercrime is estimated to cost approximately 6 trillion US dollars every year [11]. This figure is anticipated to increase as more devices connect to the internet on a daily basis. Cyberspace is increasingly becoming the *centre of gravity* for criminal activities.

Analysis of literature suggests that significant efforts have been made to develop digital forensics to respond to both existing and emerging issues relative to the application of computer sciences and law for the purpose of justice. Despite these efforts to organise digital forensics as a scientific discipline, existing models and standards do not adequately address the issue of digital evidence admissibility as these models are fundamentally investigative-oriented in scope [12] [13]. The problem of admissibility of digital evidence in the context of judicial proceedings is largely unresolved by existing research owing to the lack of a harmonised digital evidence assessment framework, which addresses the *techno-legal dilemma* underlying the application of digital evidence.

The need for a harmonised techno-legal foundation to assess digital evidence admissibility in judicial proceedings is the core motivation for this research. This research is driven by the need for a judicial tool that addresses the *techno-legal dilemma* in assessing digital evidence admissibility in judicial proceedings. The research is expected to contribute to current developments in digital forensics standardisation.

The next section of this chapter examines the problem statement and key research questions arising from the research theme.

1.3. Problem Statement

The question of digital evidence admissibility remains one of the key issues arising from the application of digital forensics in legal proceedings. The criminal justice sector is confronted not only with the increased need to investigate the rising number of crimes committed using digital tools and channels but is also overwhelmed by the challenge of producing evidence that is admissible in court [1]. Digital evidence has its peculiar challenges and its admissibility in a court of law is dependent on a number of factors and requirements.

According to one of the earliest and most important studies in the field of digital forensics and digital evidence [14] , a forensic examiner must possess the technical abilities and legal authorisation to acquire digital evidence since the entire digital forensics process embodies both legal and technical problems. This assertion explains the fact that the production of digital evidence and its admissibility in a court are essentially impacted by both technical and legal requirements. This techno-legal foundation of digital evidence has also been highlighted by other researchers [3], [15]. The idea that digital evidence admissibility in judicial proceedings is dictated by specific technical and legal requirements presents a techno-legal dilemma; the challenge or the existing gap of establishing a balanced interdependent relationship between technical and legal requirements for the purposes of establishing digital evidence admissibility and determining the evidential weight of digital evidence in judicial proceedings.

Resolving this *techno-legal dilemma* implies establishing the techno-legal foundation of digital evidence admissibility. It further implies establishing a harmonised framework that is capable of operationalising the existential interdependent relationship between the technical requirements and legal expectations. To resolve this *techno-legal dilemma*, this research addresses the central research question: *'What reproducible and standardised framework integrates both technical and legal determinants to establish the admissibility of digital evidence in legal proceedings?* In order to address the above central theme of the research, the following sub-research questions have been raised:

1. *What technical determinants underpin the admissibility of digital evidence?*

Digital forensics is a scientific discipline and therefore it is subject to specific technical processes and activities. These specific technical activities and processes, known as technical determinants**,** are assessed during trials to provide the scientific foundation for digital evidence admissibility. These determinants are derived from industry standards, academic research, legal precedents and expert opinion among other sources. The research aims to establish these technical determinants.

2. *What legal determinants underpin the admissibility of digital evidence?*

In every jurisdiction, there are legal requirements that provide the basis for the admissibility of digital evidence in a court of law. Both substantive and procedural legislations make provisions for evidence admissibility. The application of law in the criminal justice sector, irrespective of the crime typology and the legal jurisdiction of its application, has unique protocols. These protocols constitute the legal determinants for the admissibility of digital evidence. This study therefore aims to identify these determinants, which provide the legal foundation for digital evidence admissibility.

3. *What is the relationship between technical and legal determinants in establishing the admissibility of digital evidence?*

Determining the admissibility of a piece of digital evidence is essentially an assessment of the interactions and relationships between the technical and legal determinants outlined above. In other words, technical determinants impact legal determinants and vice versa. The integration of both technical and legal determinants provides a foundation for a harmonised framework to assess digital evidence admissibility. The output generated from the interactions among technical and legal determinants constitutes the basis to establish digital evidence admissibility. It is important to emphasize that cross examination as a practice associated with criminal trials, is an important judicial practice, which contributes significantly to the assessment of both the technical and the legal determinants.

4. *What are the determinants of evidential weight of a piece of digital evidence?*

The technical and legal determinants outlined above have bearings not only on digital evidence admissibility but also in determining the evidential weight of a particular piece of evidence admitted in court. Each technical and legal determinant has its bearing on a particular piece of evidence. For example, even though the lack of a digital forensics lab to conduct investigations in a quality-assured environment (i.e., a technical determinant) may impact the outcome of a case involving digital evidence, failure to document and track the chain of custody of a particular digital exhibit or a piece of digital evidence (i.e., a legal determinant) could have a more significant impact on the evidence than the former, as this could considerably affect the evidential weight of digital evidence associated with a case before a court of law. The determination of evidential weight of a piece of evidence and how both technical and the legal determinants impact this process forms a significant element of this research.

5. *How is the evidential weight of digital evidence determined?*

Evidential weight is a weight that a judge will usually attach to any evidence that is presented during court proceedings. After identifying the specific factors that underpin each of the technical and legal determinants, the research is expected to further establish the foundations of evidential weight determination as it pertains to digital evidence. Evidential weight determination constitutes an important element of this study because any judicial decision is significantly dependent on the evidential weight ascribed to a particular digital evidence tendered in court.

The next section of this chapter introduces the research methodology adopted to operationalise this research.

1.4. Research Methodology

In order to operationalise this research, the researcher adopted and conducted a number of research-based methodologies and activities as summarised in Figure 1.1.

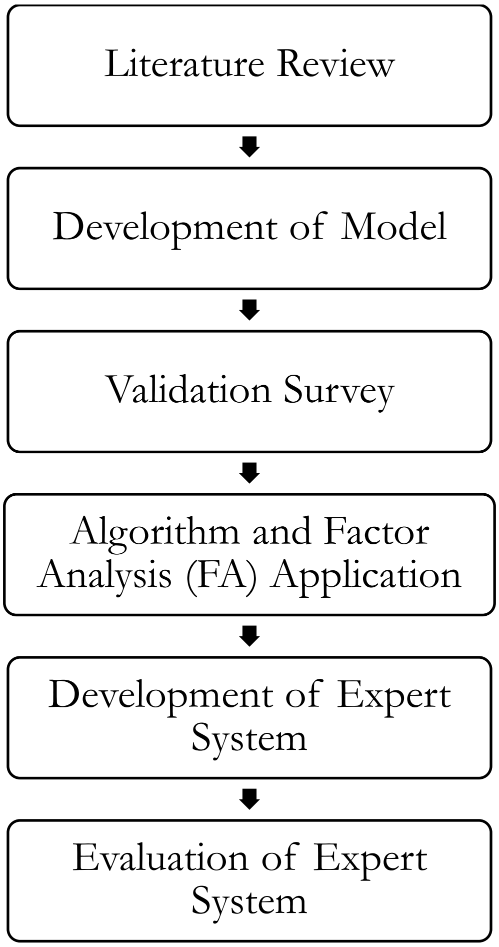

Literature Review
Development of Model
Validation Survey
Algorithm and Factor Analysis (FA) Application
Development of Expert System
Evaluation of Expert System

Figure 1.1: Research Methodology

The researcher conducted an extensive review of literature on digital forensics and digital evidence. Subsequently, the researcher developed a model representing the integration of technical and legal determinants of admissibility of digital evidence. The model developed formed the basis for the harmonisation of both technical and legal determinants, a core operation underlying this research.

In order to validate the model adopted for the study, a validation survey was conducted. Questionnaires were administered to respondents who were mainly judges but also other representatives from the criminal justice sector including investigators, prosecutors and defence lawyers. The researcher adopted a mathematical representation of the framework using Factor Analysis (FA). The researcher adopted FA to transform results from the survey into mathematical attributes, which formed the basis to operationalise the determination of evidential weight of digital evidence.

Since the scope of the research is both theoretical and practical in nature, the researcher developed an expert system — a software application based on the model introduced. The final phase of the research involved the application of the expert system developed as part of the evaluation of the model introduced to resolve the *techno-legal dilemma* introduced as the research problem. The next section addresses key terminologies and acronyms adopted for this research.

1.5. Terminologies and Acronyms

The researcher has provided definitions for key terminologies and acronyms used in this research. This has been done to support readability and understanding of the thesis. Appendix A provides acronyms adopted whilst Appendix B provides a definition of terminologies used in this research. Italicized texts are also explained in Appendix B. The next section outlines the organisation of the thesis.

1.6. Thesis Layout

This thesis is structured into six main parts comprising a total of eleven chapters as presented in Figure 1.2.

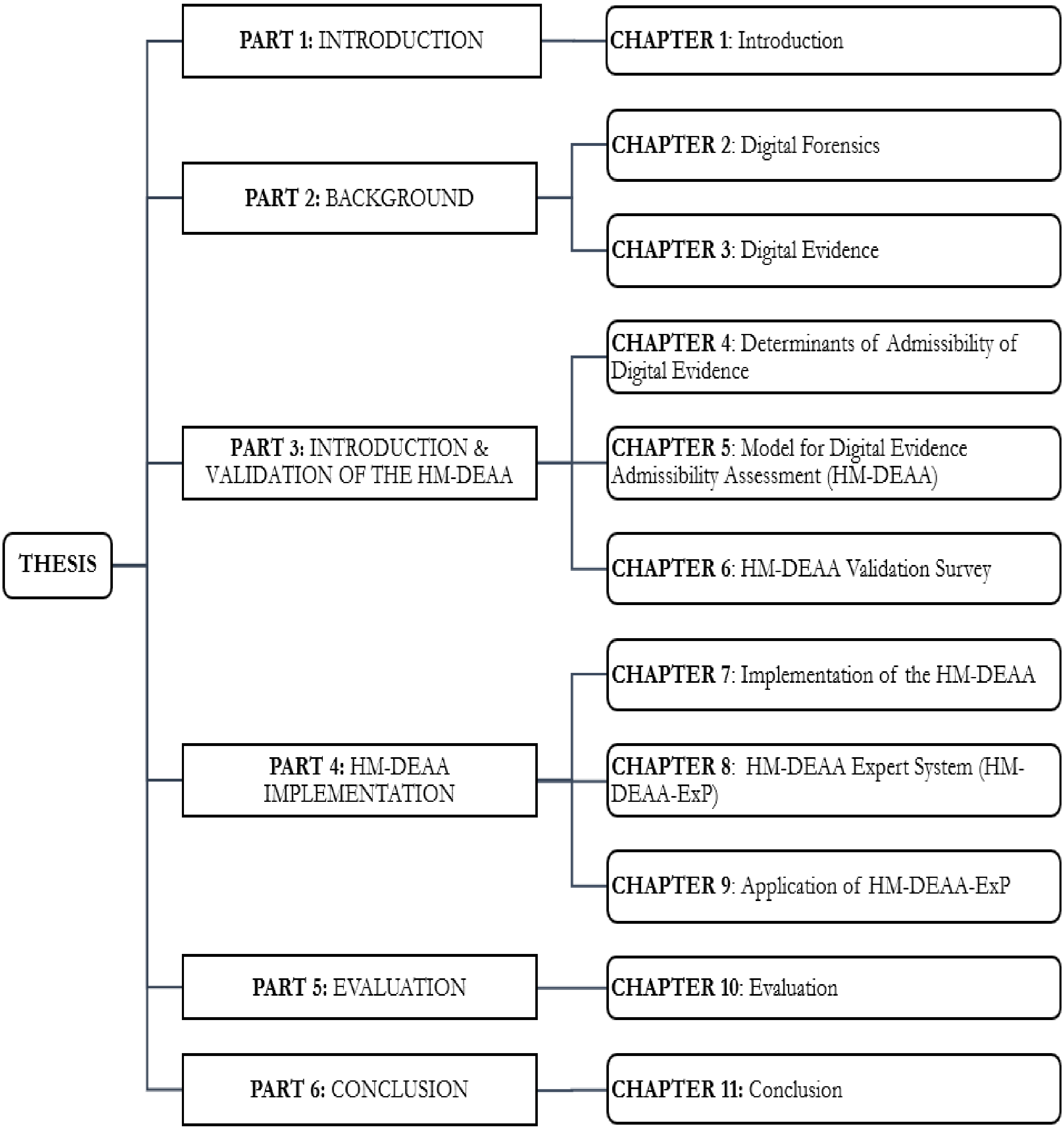

THESIS
PART 1: INTRODUCTION
CHAPTER 1: Introduction
PART 2: BACKGROUND
CHAPTER 2: Digital Forensics
CHAPTER 3: Digital Evidence
PART 3: INTRODUCTION & VALIDATION OF THE HM-DEAA
CHAPTER 4: Determinants of Admissibility of Digital Evidence
CHAPTER 5: Model for Digital Evidence Admissibility Assessment (HM-DEAA)
CHAPTER 6: HM-DEAA Validation Survey
PART 4: HM-DEAA IMPLEMENTATION
CHAPTER 7: Implementation of the HM-DEAA
CHAPTER 8: HM-DEAA Expert System (HM-DEAA-ExP)
CHAPTER 9: Application of HM-DEAA-ExP
PART 5: EVALUATION
CHAPTER 10: Evaluation
PART 6: CONCLUSION
CHAPTER 11: Conclusion

Figure 1.2: Thesis Layout

Part One of this thesis comprises Chapter 1, which introduces this research. This chapter discusses the motivation for the study and introduces the research problem. Research methodology, terminologies and the organisation of the thesis are presented in this chapter.

Part Two of this thesis covers the research background. This part covers Chapter 2 to Chapter 3. Chapter 2 provides an in-depth background information on digital forensics as a forensic science and explores previous works in the area. Chapter 3 discusses the concept of digital evidence as well as issues related to the admissibility of digital evidence in judicial proceedings.

Part Three of this thesis discusses the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA). This part covers Chapters 4 to Chapter 6. Chapter 4 discusses the technical and legal determinants of admissibility of digital evidence. Chapter 5 examines the HM-DEAA model by integrating both the technical and legal determinants into an integrated framework. Chapter 6 discusses the survey conducted to validate the HM-DEAA model.

Part Four of the thesis covers the implementation of the HM-DEAA in Chapters 7 to 9. Chapter 7 provides the mathematical foundation of the HM-DEAA through the introduction of an algorithm and the application of Factor Analysis (FA) to operationalise the model. Chapter 8 introduces an expert system developed to automate the function of the model proposed. Chapter 9 discusses the application of the expert system to real judicial cases.

Part Five of the thesis deals with the evaluation of the research in Chapter 10. The chapter discusses research contributions of the thesis and the drawbacks of the model proposed. This chapter also anticipates future work in the area in an ever-evolving information technology environment.

Part Six of the thesis contains the final chapter, which collates the conclusions of the research. The chapter recaps the central theme of the research by revisiting the problem statement and the key research questions addressed in the thesis.

In addition to the above, a bibliography of referenced works and appendices are provided to augment the entire research work. The next section concludes this chapter.

1.7. Conclusion

This chapter has introduced this thesis with an overview of the research. The research question has been framed as a *techno-legal dilemma* relative to digital evidence admissibility and evidential weight determination. This chapter has also presented the various research questions arising from the problem statement, the motivation for the study and the methodology adopted to conduct the research. The organisation of the thesis has also been described.

The next two chapters of the thesis discusses the background to this research with a specific focus on digital forensics and digital evidence.

PART 2: RESEARCH BACKGROUND

Part Two of this research covers the research background. Discussions relative to the background span Chapters 2 and 3. Chapter 2 provides detailed background information on digital forensics as a forensic science and explores previous works in the field. Chapter 3 explores the concept of digital evidence as well as issues pertaining to the admissibility of digital evidence in legal proceedings.

CHAPTER 2: DIGITAL FORENSICS

2.1. Introduction

Digital forensics has gained prominence in research due to the increasing spate of cybercrime as a result of information technology developments. The relevance of digital forensics is also influenced by the fact that computer systems are being used by criminal actors to facilitate traditional crimes such as terrorism and money laundering. In addition, as cyber-attackers increasingly target critical national information infrastructures, digital forensics has become an essential component of national response strategies to deal with escalating cyber threats.

This chapter examines the background of digital forensics with specific reference to the definition of digital forensics, the nexus between digital forensics and traditional forensic sciences, and existing digital forensics models and frameworks. The chapter also discusses digital forensics readiness and its impact on jurisprudence. The remainder of the chapter is constructed as follows: Section 2.7 introduces the concept of forensic-by-design. Section 2.8 examines existing and emerging challenges associated with digital forensics practice. Section 2.9 concludes the chapter with a summary.

2.2. What is Digital Forensics?

Digital forensics refers to the methodical recovery, storage, analysis and presentation of digital information [16]. According to the Council of Europe Electronic Evidence Guide [17], digital forensics is a branch of forensic science that deals with the acquisition, processing, analysis and reporting of evidence which is stored on computer systems, digital devices and other storage media with the aim of admissibility in court. Digital forensics has been recognised as a science in the research community. For example, Pollitt [15] defines digital forensics as 'the application of science and engineering to the legal problem of digital evidence'. According to Pollitt's assertion, digital forensics is essentially a synthesis of science and law.

Digital forensics is normally considered within the broad domain of forensic science. According to the American Academy of Forensic Sciences [18], forensic science has been in existence for the last three centuries. The Oxford Dictionary [19] traces the origin of forensics to the Latin word *forēnsis,* which it defines as the scientific process of collecting and examining information to be used as evidence in a court of law. Saferstein [20] makes references to several domains of forensics, including toxicology, chemistry and biology. He defines forensics as the application of science to the detection, examination and presentation of evidence in legal proceedings.

Practitioners and researchers have adopted different terminologies such as digital forensics, computer forensics and digital investigations to explain the scientific method of obtaining and applying digital evidence for the purpose of justice. While the term 'computer forensics' provides a narrow definition as presented by Gottschalk et al. [21] and Kuchta [22], the term 'digital investigations' is broader in scope and has been adopted by ISO in ISO/IEC 27043 [10].

Palmer [23] adopts the term digital forensics and defines it as *the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorised* *actions shown to be disruptive to planned operations.* Both Casey [3] and Cohen [24] agree that digital forensics is a typology of forensic science that relates to the identification, preservation, acquisition, examination, analysis, and reporting and presentation of evidence obtained from digital sources. Similarly, Jordaan [25] provides a normative definition for digital forensics and explains that digital forensics relates to the process of discovering evidential fragments, as well as acquiring, examining and analysing digital evidence using scientifically proven methods.

In order to comprehend the concept of digital forensics, it is essential to look into one of the earliest studies in the field. In 1995, Pollitt [14] defined digital forensics with four functional phases, namely acquisition, identification, evaluation and admission of digital records as evidence. To him, digital forensics poses a legal problem because, for example, digital evidence must be acquired within the ambit of the law in order to be admissible in a court of law. Digital forensics is also a technical problem because a forensic investigator must possess the technical knowledge and means to acquire and present digital evidence. This classic exposition by Pollitt validates the techno-legal foundation of digital forensics as a forensic science.

The existence of different terminologies to explain the scientific method of obtaining and applying digital evidence for the purpose of justice can be traced to the origin and development of computer systems and digital devices. For example, the term computer forensics itself is historic as it traces back to the earliest application of scientific methods to retrieve evidence from standalone computer systems. The adoption of the term digital forensics has been substantiated by a number of researchers. For example, Grobler and Louwrens [26] argue that due to the multitude of digital devices that exist in addition to computers, "computer forensics has become a subset of digital forensics". This implies that the term digital forensics represents the application of scientific methods across the entire digital domain for the purpose of obtaining and applying digital evidence in legal proceedings. Similar to the views held by Grobler and Louwrens [26] and a number of other researchers, including Casey [3] and Cohen [24], the researcher has adopted the terminology of digital forensics for this thesis.

The next section of this chapter traces the foundation of digital forensics as a forensic science and the nexus between digital forensics and other forensic science disciplines.

2.3. Locard's Exchange Principle and Digital Forensics

Digital forensics as a scientific discipline is rooted in the classic forensic principles. The goal of any forensic scientific method is to trace the trails that offenders leave at crime scenes and to connect offenders to the commission of the crime. Forensics is employed to obtain tangible and compelling evidence relative to the commission of a crime. *Locard's Exchange Principle* is the foundational principle of any forensic science discipline.

According to *Locard's Exchange Principle*, contacts between two persons, items or objects will result in an exchange [3]. Edmond Locard, a 20th century French criminologist postulated this principle, which pioneered the development of modern forensic sciences. This principle applies to any contact at the scene of the crime, including between a perpetrator and victim, between a perpetrator and the tool used to commit the offence, and also a trace between the crime scene and the tool used to facilitate the crime. This exchange or transfer among entities involved in the commission of a crime occurs in the physical world for traditional crimes. In digital forensics, the exchange or transfer also occurs in the digital environment.

Digital forensics as a forensic science is proven by *Locard's Exchange Principle*. A case example is presented below. For a device such as a laptop to be connected to a protected wireless network, it will need to make its Media Access Control address available to the wireless network administrator (router) before access is granted. An exchange occurs between these two devices and traces are left (the router keeps logs of the wireless internet access) after the connection. Generally, users of computer devices leave digital traces usually called digital footprints. Digital forensic examiners are able to identify suspects of computer crimes by identifying and analysing these digital footprints.

Casey [3] further expands *Locard's Exchange Principle* by categorizing exchanges between suspects and crime scenes into class characteristics and individual characteristics. According to Casey's argument, class characteristics are common traits among a similar group whereas individual characteristics are uniquely linked to a particular person or activity. According to Casey [3], the principle of individualization of crime scene transfers and exchanges applies to both traditional and digital crime investigations. Casey [3] further provides persuasive examples to substantiate his argument. In his view, a forensic examiner may be able to determine that a Microsoft Word document is fake because it may have been created using a version of Microsoft Word that was released after the purported creation date of the document in question. This is a typical example of class characteristics of evidence exchange. For individual characteristics, a forensic examiner may be able to link a Microsoft Word document to a suspect because the metadata of the document under investigation bears the unique details of the suspect.

According to Pollitt [15], the nexus between science and matters of law dates back more than 100 years. Interactions between the various scientific disciplines and legal proceedings have shaped the criminal justice system in these years. During the same period, *Locard's Exchange Principle* has also influenced a number of forensic scientists and researchers to develop new understandings of evidence and its impact on criminology as a whole. Inman and Rudin [27] have argued that forensic science follows four processes, namely: identification, classification/individualization, association and reconstruction. In digital forensics, event reconstruction is a common occurrence. For example, it is a common practice to reconstruct incident timelines through analysis of metadata information as well as file systems and communication protocols when conducting digital investigations [28]. Casey [3] and Palmer [23] argue that all forensic science disciplines follow fundamental forensic processes because these disciplines, like digital forensics are subject to the same forensic principles. Some of these forensic principles include objectivity and repeatability, which are further discussed in Section 3.5.

The next section of this chapter briefly examines the different categories of digital forensics

2.4. Digital Forensics Categories

Digital forensics is undoubtedly the newest of the forensic sciences. New developments and evolution in the information technology environment have further widened the scope of digital forensics, leading to the emergence of a number of sub-branches. This implies that the current taxonomy in digital forensics is significantly influenced by the scope of a particular digital investigation. There is currently no standardised research-based classification for digital forensics. The researcher presents below the most common forms of digital forensics within the industry and the research community. Figure 2.1 depicts the main categories of digital forensics based on the scope of its application:

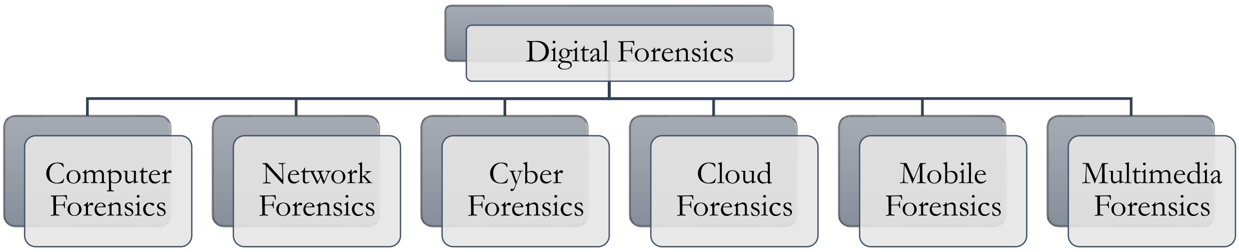


Figure 2.1: Digital Forensics Categories

Computer Forensics: This is a branch of digital forensics that pertains to the identification, preservation, collection, analysis and reporting of evidence found on computers, servers, laptops and other storage media. Computer forensics is the oldest of the categories in the above classification framework. The sub-categories of computer forensics are post-mortem forensics (autopsy), live forensics, application forensics and hardware forensics.

Network Forensics: Network forensics has gained significant prominence because of a proliferation of networks to facilitate communication and information sharing. Network forensics deals with digital evidence that is transmitted or stored over a network (wireless or wired, internet or a local area network). This domain of forensics deals with the monitoring, capturing and analysis of network traffic for digital evidence. Network forensics is an integral component of forensic readiness, especially in the corporate sector. It helps an organisation to discover the source of security attacks and intrusions targeting a network.

Cyber Forensics: Cyber-based investigations into suspected criminal activities are among the most common forms of digital investigations. Cyber forensics is the application of digital forensics processes to obtain evidence from internet sources. An alternative term for cyber forensics is internet forensics. This includes evidence from websites, social media platforms, chat forums and blog posts, among others. In recent times, cyber forensics has been applied to investigate suspected criminal cases on the dark net as this new but 'hidden' network has become one of the fertile grounds for transnational criminal activities.

Cloud Forensics: Cloud forensics is essentially the application of digital forensics in a cloud computing environment. Forensics in the cloud environment involves interactions among several cloud actors (i.e., cloud provider, cloud consumer, cloud carrier, etc.) for the purpose of facilitating investigations. Cloud evidence is mostly subjected to legal issues as evidence obtained from the cloud computing environment may be located in a different legal jurisdiction.

Mobile Forensics: This domain of forensics has emerged as a result of the growth and popular use of mobile devices, including cell phones and smart devices. More people are connecting to the internet through their smart devices than with their normal computers. The availability of social media and communication applications on handheld smart devices has contributed to the increasing relevance of mobile forensics to the criminal justice actors.

Multimedia Forensics: This is a branch of digital forensics that deals with the collection, analysis and forensic evaluation of photographic images as well as sound and video recordings. This domain of forensics deals with establishing the authenticity of an image, an audio or video recording and to determine any tampering, whether intentional or by accident. Data pertaining to multimedia files are becoming a recognised group of forensic artefacts due to the proliferation of such files in recent times [29].

New sub-domains in digital forensics are likely to emerge in response to emerging forensic requirements due to the continuous evolution of the information technology ecosystem. Classification of the various digital forensics types is important because such a taxonomy affects the choice of forensic model or approach used for a particular digital investigation. Digital forensics models are presented in the next section.

2.5. Digital Forensics Models and Frameworks

According to Leigland and Krings [30], digital forensics processes and techniques were generally fragmented. Approaches for gathering digital evidence were developed ad-hoc by investigators, especially within law enforcement. Personal experiences in digital investigations and expertise developed over a period of time guided the development of ad-hoc investigations models and guidelines [30].

There have been several proposed models aimed at rationalizing digital forensics processes and procedures. Digital forensics models are important because they do not only help to explain the steps involved in the recovery of digital evidence, but they also provide operational guidance for the effective processing of digital evidence in a forensically sound manner. Arshed et. al [29] have argued that, the lack of unified processes and procedures impact negatively on the contributions of digital evidence in legal proceedings. The models ensure that each digital forensics activity follows an acceptable and proven forensic methodology. Table 2.1 provides a summary of proposed scientific models for digital forensics.

Table 2.1: Existing Digital Forensic Investigation Process Models [31]

SN	Year	Model/Framework	Author (s)	Phases
1.	2001	National Institute of Justice (NIJ)	Ashcroft	5
2.	2001	DFRWS Model	Palmer	7
3.	2002	Abstract Digital Forensic Model	Reith, Carr & Gunsch	9
4.	2003	The Integrated Digital Investigative Process	Carrier & Spafford	17
5.	2004	Enhanced Digital Investigation Process Model (EDIP)	Baryamureeba & Tushabe	4
6.	2004	An extended Model of Cybercrime Investigation	Ciadhuain	13
7.	2004	A Hierarchical, Objectives-Based Framework for the Digital Investigations Process	Beebe & Clark	6
8.	2006	Framework for a Digital Investigation	Kohn, Eloff & Oliver	4
9.	2006	The Four-phase Forensic Process	Kent, Chevalier, Grance & Dang	4
10.	2009	Digital Forensic Model based on Malaysian Investigation Process	Perumal	7
11.	2011	The Systematic Digital Forensic Investigation Model	Agarwal	11
12.	2012	Harmonised Digital Forensic Investigation Process Model	Valjarevic & Venter	12

Development and adoption of models as a way of formalizing digital forensics as a scientific discipline is directly linked to the earlier development of digital forensics. One of the earliest attempts towards digital forensics harmonisation was the Digital

Forensics Research Workshop held in 2001. The research workshop produced a digital forensic process model that consisted of seven phases [4]. This included identification, preservation, collection, examination, analysis, presentation and design.

Other models were subsequently developed by law enforcement and researchers. For the purposes of this research, the researcher further explains the models, which are widely cited in literature. Reith et. al. [5] proposed the 'abstract model' of digital forensics. The Association of Chief Police Officers' Good Practice Guide [7] and the U.S. Department of Justice Electronic Crime Scene Investigation Guide [8] are examples of efforts by law enforcement actors to harmonise digital forensics and provide a common approach to conduct digital investigations.

The U.S. Department of Justice Electronic Crime Scene Investigation [8] proposed a five-phase digital forensics process model, which consists of the following:

1. Collection: Includes evidence search, evidence recognition, evidence collection and documentation.
2. Examination: Involves the facilitating the visibility of evidence before analysis.
3. Analysis: The processing of available electronic information for significance and probative evidential value to the case under investigation.
4. Reporting: Report detailing the examination process and forensic findings.
5. Presentation: Presenting evidence findings in support of legal proceedings.

Zimmerman and Glavach [32] have also proposed digital forensics as a distinctive four-phased process, similar to the other models proposed. The four phases of the model are:

1. Collection of digital artefacts (exhibits) in a forensically sound manner.
2. Preservation of artefacts in a forensically sound manner.
3. Filtering/analysis for potential evidential value.
4. Presentation of digital evidence.

Other works aimed at standardising digital forensics have been carried out by various researchers. Valjarevic and Venter [6] have proposed a harmonised digital forensic model aimed at resolving the various fragmentations associated with previous digital forensics processes. The Scientific Working Group on Digital Evidence has published various guidelines covering specific incident investigations [33]. In 2011, Agarwal [34] proposed the Systematic Digital Forensic Investigation Model. The model proposed has the following phases: preparation, securing the scene, survey and recognition, scene documentation, communication shielding, evidence collection, preservation, examination, analysis, presentation and review.

The growing importance of Internet of Things (IoT) and cloud computing has led to the introduction of specific models to address investigation challenges arising from recent technological developments. Perumal et al. [35] have introduced IoT-Based Digital Forensics Model which defines a standard operating procedure for investigations targeting IoT devices. Harbawi and Varol [36] have also proposed a theoretical framework for IoT-based forensics which addresses digital evidence acquisition issues. Cloud-based digital forensics frameworks have also been introduced [37], [38], [39]. In addition, Ab Rahman et al. [40] have introduced a forensic-by-design framework for Cyber-Physical Cloud Systems. The framework covers risk management principles and practices, forensic readiness principles and practices, incident handling principles and practices, laws and regulations, hardware and software requirements as well as industry-specific requirements.

Due to the increasing forensic challenges with big data especially with regards to volume and data complexity, researchers have introduced additional frameworks to enhance digital forensics procedures pertaining to big data investigations. Adedayo [41] has proposed a digital forensics framework to enhance better collection, analysis, preservation and presentation of digital evidence pertaining to big data. Similarly, Mohammed et. al. [42] have introduced an automated framework for forensic analysis of heterogeneous big data.

Standardisation of digital forensics achieved a major milestone when the International Organization for Standardization (ISO) published standard ISO/IEC 27037 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence in 2012 [9] and standard ISO/IEC 27043 — Incident Investigation Principles & Processes in 2015 [10]. Both standards provide guidelines for various incident investigations.

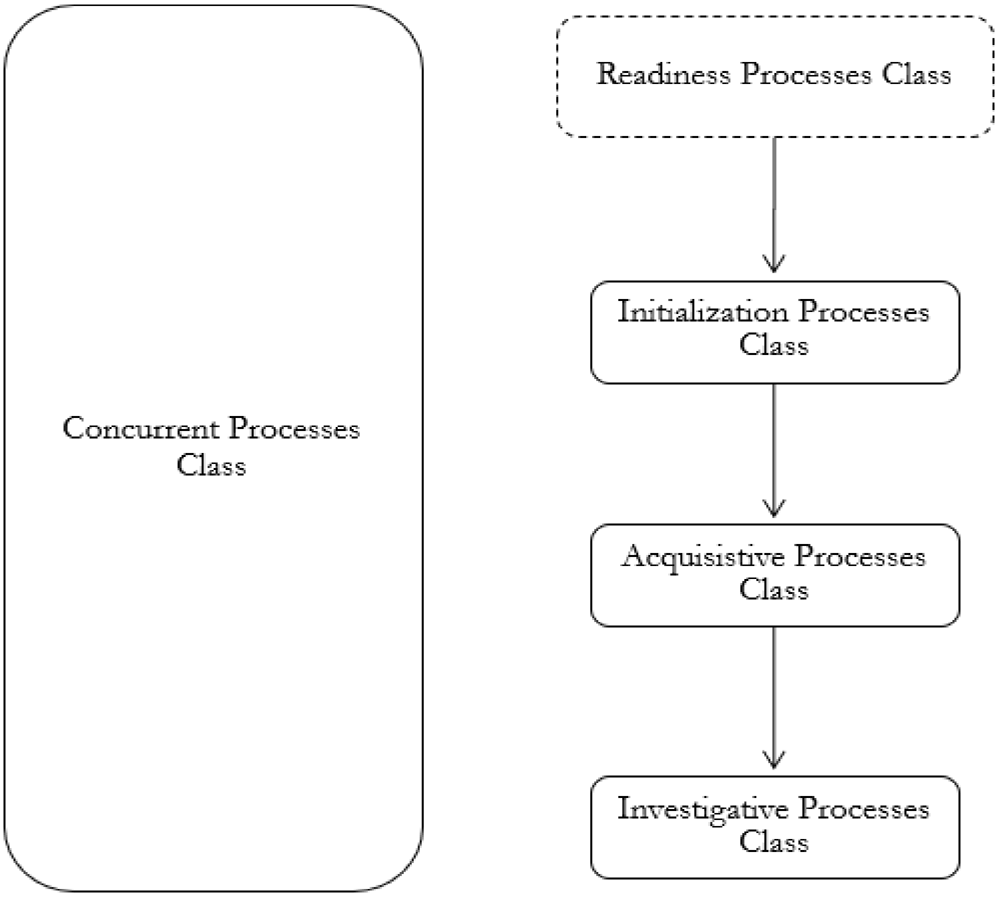

Concurrent Processes Class
Readiness Processes Class
Initialization Processes Class
Acquisistive Processes Class
Investigative Processes Class

Figure 2.2: Classes of Digital Investigation Process (Source: ISO/IEC 27043:2015)

Critical examination of literature covering the subject matter suggests that, these approaches and models have contributed significantly to digital forensics standardisation both in research and in practice. However, the approaches and frameworks presented are largely applied to investigation processes rather than in the context of judicial proceedings [12], [13]. The application of these approaches is therefore limited in scope relative to the assessment of digital evidence admissibility in judicial proceedings.

The next section of the chapter examines an emerging area of digital forensics, which has transformed the traditional view and treatment of digital forensics as a reactive forensic discipline.

2.6. Digital Forensics Readiness

Digital forensics readiness has received significant research attention in the last decade. This significance has manifested not only in the corporate information security environment, but also in literature. Researchers, including Valjarevic and Venter [6], and Carrier and Spafford [43] have integrated digital forensic readiness into their proposed models. Their models, though focused on investigations, also recognise the forensic readiness phase as an integral component of the digital forensics process. These developments have transformed the classic notion, that viewed digital forensics narrowly as a reactive scientific methodology. According to Grobler and Louwrens [26], forensic readiness has transformed digital forensics from an investigation and response mechanism towards a more proactive approach of obtaining and applying digital evidence in matters of justice. Digital forensics readiness brings to bear the proactive dimension of digital forensics and this is especially significant in corporate digital forensics practice.

Digital forensics readiness activities include defining business and incident scenarios, identifying potential digital evidence sources, forensic handling of data representing potential digital evidence, planning incident detection, defining and implementing system architecture for forensic readiness, and installing software and hardware solutions to support the process of incident detection and forensic response. Tan [44], one of the earliest researchers in the field introduced the concept of forensic readiness to cover two practical objectives — maximizing an environment's preparedness to collect admissible digital evidence and minimizing costs associated with post-incident investigations. Consequently, Rowlingson [45] defined forensic readiness as the ability of an organisation to maximize its potential, through technical and non-technical means to use digital evidence while minimizing the costs of an investigation.

From the above concept of forensic readiness, Rowlingson [45] has outlined a number of benefits for an organisation that develops its forensic readiness. Some of the benefits include effective evidence gathering to support an organisation's defence in case of a lawsuit, improving deterrence of insider threats, effective incident response operations with minimal business disruptions and facilitation of a systematic approach to evidence collection, which will enhance the forensic soundness of digital evidence.

It is essential to highlight that digital forensics readiness does not only serve a business purpose; in the corporate environment, it also helps to address some critical challenges associated with digital forensics. For example, the ability to collect network traffic for analysis is significantly enhanced in a forensically ready network environment rather than applying traditional forensics investigations into a network security breach in an environment with no or minimal forensics readiness. Thus, even though digital forensics readiness is normally considered in a corporate environment, the concept and deployment of forensic readiness activities complement and enhance law enforcement investigations, especially when such activities are backed by law and corporate policy.

The inclusion of digital forensic readiness in this research is important for two principal reasons. As an emerging dimension of digital forensics, which has already shaped our traditional view of digital forensics, it is essential that forensics readiness is recognised and integrated into current and future digital forensics standardisation efforts. In addition, it is essential to consider forensic readiness and apply the same rules of evidence to the operationalization of digital forensic readiness activities to ensure that evidence collected from such activities are fit for purpose. This is essential as corporate level investigations may end up in a court of law. These two reasons are central to the development and operationalization of an integrated model that provides a techno-legal foundation for establishing the admissibility of digital evidence as the research seeks to establish.

Due to the increasing relevance of forensic readiness in digital forensics, researchers have introduced an enhanced concept of forensic readiness called 'forensic-by-design' to increase the potential use of digital evidence while decreasing the costs and the barriers to investigations. The next section discusses this concept and its relevance to digital forensics.

2.7. Forensic-by-Design

Researchers have introduced a new concept — forensic-by-design to further enhance the potential to retrieve and utilize digital evidence when a breach occurs [46], [40]. The introduction of forensic-by-design and its application in different environmental contexts has further enhanced the concept of forensic readiness. It is important to emphasize that the scope of forensic-by-design systems is not to prevent cyber-attacks or security incidents. Forensic-by-design systems are meant to improve the forensic environment of a system or a target computing environment by improving investigations response. For example, a forensic-by-design system will enhance incident response and investigations through preservation of evidential information in a target environment such as a cloud system.

Ab Rahman et. al. [46] define forensic-by-design as a concept that integrates forensic requirements into the design and development of an architecture or an IT system. A forensic-by-design model for organisational cloud users for incident investigations has been introduced by Ab Rahman et. al. [46]. The model consists of the following requirements:

1. Risk management principles and practices
2. Forensic readiness principles and practices
3. Incident handling principles and practices
4. Laws and regulations
5. Hardware and software requirements, and
6. Industry-specific requirements.

The above requirements are operationalized across six phases, namely (1) Preparation, (2) Identification, (3) Assessment (4) Action and Monitoring, (5) Recovery, and (6) Evaluation.

Similarly, Grispos et. al. [47] have introduced a forensic-by-design framework which introduces forensic readiness testing and an approach for verifying and validating forensic-by-design approaches. This framework consists of nine components, namely risk assessment, forensic readiness principles, security requirements, privacy requirements, relevant legislation, relevant regulations, medical requirements, safety requirements and software and hardware requirements.

Alenezi et. al. [48] have proposed a Cloud Forensic Readiness Framework (CFRF) which recognizes three factors, namely technical, legal and organizational factors. The technical factors consist of cloud infrastructure, cloud architecture, forensic technologies and cloud security. The legal considerations include service level agreements, regulatory requirements and jurisdiction with a recommendation for the adoption of a multijurisdictional approach. The organizational factors underpinning the CFRF include management support, readiness strategy, governance, culture, training and specific organisational standard operating procedures. Ras and Venter [49] have also introduced a theoretical architectural model to enable proactive forensics of cloud computing systems. This model establishes a correlation with ISO 27043 standard of forensic investigations.

The application of forensic-by-design concepts in system and software development has also received significant attention in literature. Research suggests that organisations have started considering such requirements in the development of IT-based systems including software development [50]. Pasquale et. al. [51] have proposed an approach to ensure software systems are forensic-ready to support digital forensics response to cyber-attacks and system breaches. Pasquale et. al. [51] further proposed a number of requirements underlying forensic readiness in a software development context. These requirements include availability, relevance, minimality, linkability, completeness, non-repudiation, data provenance, and legal requirements.

Ab Rahman et. al. [46] discuss the benefits of adopting a forensic-by-design approach in digital forensics by postulating that forensic-by-design models will provide an in-depth understanding of an incident, help identify attackers and potentially their motives, and improve response to cyber incidents. The introduction of forensic-by-design frameworks constitute a novel forensic approach in responding to the ever-evolving nature of computing and associated distributed technologies which continue to impact on digital forensics. The next section discusses the challenges associated with digital forensics.

2.8. Challenges with Digital Forensics

Digital forensics is constrained by a number of technical and legal challenges. While scientific research has led to the enactment of technology-focused legislations and the development of appropriate technology to facilitate investigations and prosecutions of cyber-dependent and cyber-facilitated crimes, several challenges still remain. Cybercrime itself, which is the object of digital forensics activities, remains a challenge to both practitioners and researchers. Unfortunately, the current trends associated with information technology developments, including the development of cloud computing, internet of things and crypto-technologies are likely to further escalate the challenges associated with digital forensics.

According to a research conducted by Fahdi et. al. [52], 93% of survey respondents indicated that the number and complexity associated with digital forensics would increase in the future. Understanding the nature of the current challenges is significantly helpful to shape not only ongoing research and discourse on the subject matter, but also to shape practical responses to the problem. While these challenges could affect the successful application of digital forensics, it is essential that research is encouraged to document these scientific challenges to orient future research in the field.

From a technical dimension, digital forensics is impacted by a number of factors, including the following: encryption technology, ever-increasing large volumes of data for forensic analysis, greater anonymity in the IT environment and other technological complexities. In addition, a number of technically-driven anti-forensic techniques have emerged that have contributed to the difficulty faced by investigators and forensic examiners. Gül and Kugu [53] discuss a number of these anti-forensic techniques including data pooling, manipulating of file signatures, restricting filenames, manipulating of MAC addresses and hash collisions among others.

Encryption technology has also become a tool of choice for cybercriminals. Criminals continue to use encryption technologies to hide their communications on the internet and to conceal their tracks when committing a crime. In recent times, cyber criminals operating in Ghana — the so-called *Sakawa* perpetrators normally use truecrypt application, which is a free encryption application, to encrypt the hard drives of the laptops that they use to perpetrate cyber fraud. In addition, Janssen [54] has observed that criminals use steganography alongside encryption to provide an additional layer of security to conceal and hide data that could be the target of investigations.

Technology for anonymous communication such as The Onion Router browsers and other internet anonymizers are freely available to aid criminals to hide their tracks. Rekhis and Boudriga [55], [53] recognise this as the most common technique of obfuscating the source of cyber-attacks. For example, if a suspect uses an anonymous e-mail client on the internet to send an e-mail, a forensic examiner will only find a false email header when investigating the e-mail. Such cases prove extremely difficult, if not impossible for even law enforcement with all available resources to successfully investigate. Even though some of these technologies are effectively privacy enhancing tools, their criminal use has become problematic for legitimate investigations work.

Mobile device also presents its unique challenges to law enforcement and investigators. It continues to record significant growth especially in developing countries due to the increasing connectivity. Mobile devices include a variety of digital devices with different and most often, proprietary operating systems. Different operating systems may require different tools and skillset to obtain forensic evidence. A significant amount of data associated with mobile devices may never be stored on the mobile device itself because of the availability of cloud based-applications that provide storage service for users [56]. Newer versions of mobile devices have enhanced security mechanisms such as remote data wiping functionalities installed. Once this functionality is effectively activated by a suspect, it could lead to loss of valuable evidence. Other mechanisms which could impact on the ability to retrieve evidence from mobile devices include the use of biometric and encryption technologies which are meant to safeguard privacy of users.

A number of challenges are encountered when conducting investigations in the cloud environment [57]. These include difficulty or lack of the possibility to physically assess servers and cloud computing devices, location of cloud devices (usually in another jurisdiction) and technical difficulty in obtaining metadata information [58]. According to Arshed et. al. [29], cloud architectures are generally distributed. This makes forensic acquisition and analysis difficult during investigations.

With regards to Unmanned Aerial Vehicles (UAVs) and driverless vehicles, forensic investigators encounter a number of challenges. Since the technology underlying UAVs and driverless vehicles are relatively new, law enforcement will require new knowledge and tools to be able to conduct fit-for-purpose investigations into these systems. Existing forensic processes and tools may not be sufficient to conduct forensics into these automated systems because of the variation and the proprietary nature of UAVs and automated vehicles. In addition, information can be stored in several locations and sources and this may add additional layer of challenge to investigators [59].

IoT technology has further created additional challenges for law enforcement and investigators [57]. Alabdulsalam et al. [60], [36] have raised some of these challenges. The issue of IoT evidence location is critical in digital forensics as IoT data may be located in different sources, including cloud, mobile devices as well as other third-party locations. The proprietary nature of IoT devices has ballooned these challenges as most of these devices have different operating systems and communication protocols [60]. MacDermott et al. [61] have also raised issues with forensic data acquisition in IoT devices. Digital evidence in IoT environment is highly volatile as most of these devices have limited storage capacities to keep information of evidential value for a long time. This situation could lead to loss of evidence even when a crime has been committed in an IoT environment.

These newer sources of digital evidence pose new and challenging problems across the digital forensics chain for law enforcement and investigators.

Despite the continuous review of legislations to accommodate technological advances and their impact on cybercrime and digital forensics, several legal challenges exist. The very nature of cybercrime as a transnational crime creates trans-jurisdictional issues for digital forensics. For example, it can be problematic for law enforcement to identify suspects and determine lawful judicial authorities to oversee a criminal trial involving multiple locations of technology actors, especially in the absence of harmonised legal frameworks. Even though the Budapest Convention on Cybercrimes [62] provides a mechanism for parties of the treaty to facilitate cross-border investigations and prosecutions, only 60 countries had acceded to this international treaty as at August 2018.

Privacy is another area of concern in the field of digital forensics. The application of human rights and data protection principles and practices in digital forensics has created problems around privacy. Consequently, law enforcement officials and forensic examiners are duty-bound to ensure that human rights and data protection principles are adhered to. The researcher has been involved in a number of investigations in which suspected criminals have cited privacy concerns as the reason for their use of ToR browsers, steganography techniques and other anonymous applications that were found installed on their computers during investigations. In the case of Edmund Addo vs the Republic of Ghana [63], a human rights court granted a relief to an applicant who took the police to court for seizing his electronic devices. The judge ruled, among other issues raised that the seizure and retention of the devices breached the suspect's fundamental human rights.

Apart from these technical and legal challenges, other challenges undermine the effective application of digital forensics. Lack of training, especially for the core criminal justice actors — judges, prosecutors and investigators remain the biggest issue confronting the operationalization of scientifically proven methods in cybercrime investigations. Lack of resources, including digital forensic laboratories and appropriate digital forensic tools, especially in developing countries has contributed to a low adoption of digital forensics best practices. These challenges may affect the effectiveness of digital forensics processes and procedures and this could, by extension, impact the quality of digital evidence produced from such investigations. The next section concludes this chapter.

2.9. Conclusion

This chapter introduced the theory and application of digital forensics and examined the various concepts of digital forensics. Based on a review of literature on the subject, the researcher provided a functional definition of digital forensics as the application of scientifically derived and proven methods for obtaining and applying digital evidence for the purpose of justice. The chapter further explained the scientific basis of digital forensics and the nexus between digital forensics and other forensic sciences through the application of *Locard's Exchange Principle*.

Different typologies of digital forensics were presented and explained in the chapter. Existing digital forensics frameworks were presented and their impacts on the research were established. Challenges confronting digital forensics as a forensic science were identified and adequately discussed in the chapter. The next chapter discusses digital evidence and its consideration in criminal matters.

CHAPTER 3: DIGITAL EVIDENCE

3.1. Introduction

Digital evidence has become considerably important because of the involvement of the internet and electronic devices in criminal activities. As technology continues to develop in scope and relevance, so does the need to rely on digital evidence in the administration of justice, be it criminal, civil or corporate level investigations. Riding on the tide of the current ICT revolution, criminals have expectedly transitioned to the use of computers, mobile devices and other digital channels to commit crimes [30]. This development requires criminal justice actors to investigate, produce and present evidence through a process that is legally admissible and capable of securing successful prosecutions.

This chapter examines the concept of digital evidence and its applications in criminal proceedings. It also examines the various types and sources of digital evidence, interrogates the differences between traditional and digital evidence, and explores the principles underlying the application of digital evidence in judicial matters. The remainder of the chapter is structured as follows: Section 3.6 examines the various arguments on digital evidence admissibility and the challenges associated with its application. Section 3.7 concludes the chapter with a summary.

3.2. What is Digital Evidence?

Digital evidence is simply a product of digital forensics [64]. According to ISO/IEC 27037 [9], digital evidence is information or data stored or transmitted in binary form that may be relied upon as evidence. Cohen [24] agrees with the above narrative and further describes digital evidence as the product of a digital forensics process. The Council of Europe (COE) [17] defines digital evidence as "any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings". Digital evidence is also referred to as electronic evidence [17], digital forensics evidence [24] or computer forensics evidence [65]. According to Mason [66] and Kerr [67], these terminologies may differ in meaning but have no formal legal relevance.

Digital evidence is a form of evidence. Researchers including Cohen [24], Casey [3] and Kerr [67] describe evidence as information that can be introduced at trial to help judges, adjudicators and juries make decisions in legal proceedings. Black's Law Dictionary [68] defines evidence as "any species of proof, or probative matter, legally presented at the trial of an issue, by the act of parties and through the medium of witnesses, records, documents, exhibits, concrete objects, etc. for the purpose of inducing belief in the minds of the court or jury as their contention". When evidence is presented, the court has to balance its probative value to determine its relevance to either prove or disprove a fact in dispute.

Ghana's Evidence Act 1975 (NRCD 323)[2] defines "evidence" as a 'testimony, writings, material objects, or other things presented to the senses that are offered to prove the existence or non-existence of a fact'. Whilst the above legislation was enacted by Parliament before computers were widely introduced in Ghana, the Electronic Transactions Act (ETA)[3] which introduced computer-generated evidence into judicial proceedings in Ghana was passed in 2008. In the ETA, digital evidence is referred to as 'electronic record' which is defined in interpretation clause as 'data generated, sent,

[2] Ghana's Evidence Act 1975 (NRCD 323) is an Act of Ghanaian Parliament which contains several provisions of much relevance to digital evidence. http://laws.ghanalegal.com/acts/id/360/section/179/Interpretation

[3] The Electronic Transactions Act, 2008 (Act 772) is an Act of Ghanaian Parliament, which provides for the regulation of electronic communications and related transactions and to provide for connected purposes. https://www.moc.gov.gh/electronic-transactions-act-772

received or stored by electronic means'.

Brobbey [69] classifies evidence into the following categories:

- *Real Evidence:* Evidence with characteristics that are directly and materially related to the case before the court. An example is a gun used by a suspect to commit murder.
- *Testimonial or Oral Evidence:* Oral information given in court, such as witness testimony.
- *Demonstrative Evidence:* Information of an illustrative nature, such as pictures, site plans and maps.
- *Documentary Evidence:* Information in written form, such as affidavits, business contracts, indentures, etc.
- *Scientific Evidence:* Technical or specialised information that is obtained through scientific methods.

Brobbey [69] therefore classifies digital evidence as a scientific evidence. However, he further argues that in the application of law, digital evidence, though classified as scientific evidence may be considered as hearsay evidence.

Generally, the rules of evidence define hearsay evidence as information or statements not made in oral evidence in court proceedings. Under the hearsay principle, digital evidence is considered as circumstantial evidence on the basis that data that originates from a computer system is considered as hearsay because it is not directly seen from the computer by anyone other than the creator of the data. Proponents of this view, such as Stephenson [70] further argue that digital evidence as a product of computer forensics is not based on personal observations. This view is intrinsically linked to the classic concept of science where direct personal observation establishes the veracity of information or an account in relation to an offence or a crime.

There is an opposing argument relative to the position of digital evidence in matters of law. For a hearsay rule to apply, the declarant has to be a human being [69]. An electronic device such as a computer, that generates digital evidence is not a human being and therefore cannot be described as a declarant. In addition, through digital forensics processes and activities, modern scientific methods help forensic examiners to establish direct links between suspects and user activities on digital devices. Cohen [24] argues that digital evidence is considered as physical evidence since in most jurisdictions, digital devices and their contents are considered as personal property for which a warrant or an order is required before search and seizure can be conducted.

Digital evidence has been used in several criminal, civil and corporate cases and its recognition and acceptance has improved in the last decade due to increasing understanding of digital forensics and changes in law to accommodate current technological developments. According to Daubert [71], digital evidence is required to meet the standards of scientific tests before it can be admitted by courts. Kessler [64] has however argued that judges' understanding of technology and digital forensics processes significantly affects their understanding and, consequently, their decisions on cases involving digital evidence.

According to Cohen [24] and Kerr [67], understanding of digital forensics processes remains a significant factor in determining the evidential weight of a piece of evidence during trials. In order to further examine digital evidence admissibility, it is essential, first of all, to discuss the typologies and sources of digital evidence.

3.3. Types and Sources of Digital Evidence

Generally, three categories of evidence are obtained from digital forensics activities. These are static data (dead box), live data and internet data. This evidence classification is determined by the target source, the state of data being collected, and the digital forensic method being employed for collection and analysis. There are a wide range of digital devices and electronic mediums that offer the potential for evidence recovery. Forensic examiners are required to consider the nature and source of the potential evidence and adopt the best forensic procedure for its preservation, collection, examination, analysis and reporting.

Static data is evidence retrieved through the application of static forensic methods. Traditionally, digital forensics is based on this static analysis. There are well established protocols for conducting static analysis. These procedures include making forensic duplicates of digital devices using write blockers, validating the forensic copies using hash algorithms, indexing forensic images before examination and eventually searching the contents of processed exhibits for potential evidence. Different forensic applications such as Encase and Forensic ToolKit (FTK) are available to perform analysis on forensic copies.

On the other hand, live data is evidence collected for live computer systems and servers. For live analysis, evidence is collected when the target system is in 'live' or 'running' mode. Typically, forensic examiners would adopt live analysis as the first step to collect evidence whenever the target computer is in active mode. This technique is also adopted in an environment where it is not practically feasible to shut down the entire system for static analysis. In conducting network intrusion investigations in an internet banking environment, it is not practically feasible to shut down the internet banking server to investigate suspected network intrusion. It is essential to highlight that in live analysis, any action performed by the forensic examiner may alter the state of the target system. Forensic examiners are required to execute actions that are forensically relevant and to document the rationales for actions undertaken.

Internet related evidence has become significantly important for investigators. Internet technologies have enabled criminal enterprise to thrive by way of communication and information sharing. Websites, chat rooms, message boards, social media platforms and other digital forums, including darknets are great sources of digital evidence for investigators. The nature of the internet's architecture and the various applications and technologies running on it make the world wide web an important repository of digital evidence. Investigators find internet sites important sources of evidence because criminals leave traces on the internet. In some cases, law enforcement conducts undercover investigations to obtain information, which is introduced to the court as evidence under the appropriate legal considerations. Evidence collection through static analysis, live analysis and internet sources may complement each other in a particular investigative case.

The various types of evidence described above can be obtained from a variety of sources. These include desktop computers, laptops, digital cameras, music players, cellular telephones, websites, e-mails, social networks and routers, logs from servers and records from telecommunication service providers. Compact discs, digital versatile discs, SIM cards, floppy disks, hard drives and memory cards are also valid sources. Digital evidence may come in the form of either user-generated data or computer-generated data. User-generated data include documents, photographs, image files, databases and financial information. Examples of computer-generated data include internet browsing history and event logs.

Current developments in computer engineering and ICT have led to newer sources of digital evidence. The advent of Unmanned Aerial Vehicles (UAVs) popularly referred to as drones, Internet of Things (IoTs), and driverless vehicles have led to new developments in digital forensics because of the potential source of digital evidence from these systems. In recent times, UAVs have become important focus for law enforcement because of their impact on safety of people and security in the airspace. Due to the popularity of their use, UAVs have become a potential source of evidence [59].

IoT represents a new technological development in the field of ICT. IoT devices store information and most of them have the ability to share information with other network-centric systems. Researchers have indicated that IoT devices were not designed with security in mind and therefore vulnerable to criminal exploitation [60]. Potential criminal use of driverless vehicles has also been cited. For example, criminals could use these automated vehicles to transport unlawful guns and drugs [72]. The potential use of driverless vehicles has heightened the relevance of obtaining digital evidence from these systems.

New digital technologies in the form of applications and services are being developed and integrated into the digital ecosystem. These developments are expected to broaden the domain of digital evidence sources. The next section of this chapter briefly examines the differences between traditional evidence and evidence obtained from digital sources.

3.4. Traditional Evidence Vs. Digital Evidence

There is no substantive difference between digital evidence and other forms of traditional evidence because both serve the same purpose [43], [73]. However, several researchers contend that digital evidence has specific characteristics that distinguish it from other forms of traditional evidence. These unique characteristics of digital evidence include its volatility, the complexity of the digital domain, large datasets and rapid changes in the technology environment that constitute the source of digital evidence [74], [75].

Other researchers, on the other hand, have argued that digital evidence is 'superior' to other forms of traditional evidence [76], [77]. This argument is grounded in the fact that digital evidence contains useful and forensically relevant data such as details of key dates, times and a history of the file or data in question [28]. Digital evidence, the argument continues, tends to provide metadata information about itself. This establishes the basis to link a suspect to a crime as well as other events and activities leading to the perpetration of a crime. According to proponents of this argument, digital records can establish not only the intent but also the ability of the suspect to commit the crime. Another important attribute of digital evidence is that unlike most forms of physical evidence, digital evidence is difficult to destroy as digital records may be recovered even if it is deleted.

The nature of digital evidence itself embodies unique characteristics that distinguish it from conventional evidence. For instance, digital evidence can easily be altered compared to conventional evidence [78]. Unless technical measures such as the use of hash functions are applied, modifications of digital evidence can be difficult, if not impossible to detect by non-technical handlers. Digital evidence is susceptible to unauthorised manipulation. According to Akester [79], inaccuracies relative to the attribution of authorship and the ability of automated programmes to create user contents on a computer device provide another basis to question the reliability of digital evidence. This existential fragility of digital evidence raises questions about the completeness, reliability and validity of the sources and creators of digital evidence. In practice, forensic examiners employ technical measures such as the use of write blockers and hash algorithms to ensure that digital records are protected from unauthorised manipulation.

Kenneally [80] has argued that digital evidence is different from documentary evidence in the area of storage, backup, copying, transmission and security. Similarly, Kessler [64] has argued that digital evidence differs from conventional evidence in that digital evidence can easily be altered with no limit to its size. In addition, digital evidence contains information on the originality of the data. Kessler [64] further argues that documentary evidence is cumbersome in nature and generally does not contain information about its originality. Digital forensics is latent in nature and hence can only be processed with specialist tools by trained personnel.

Traditional evidence has been tested by the courts for a very long time and has consequently established its standing and credibility in courts. The credibility achieved by conventional evidence is grounded not by its history alone, but also by its ability to establish a direct relationship between suspects and the commission of an offence. Digital evidence is relatively new to courts and as is explained above, its very nature reveals certain fragilities. These issues are addressed through the adoption of appropriate and rigorous scientific methods, which are underpinned by fundamental forensic principles for the preservation, collection, examination, analysis and interpretation of digital evidence. The next section examines the key principles governing digital evidence.

3.5. Principles of Digital Evidence

Efforts to rationalise digital forensics practice as a forensic science begun with the formulation of certain scientific principles. These principles provide a common scientific approach for the handling of digital evidence in order to meet its intended purpose. Early forensic practitioners realised that the existential fragility of digital evidence could only be addressed through a set of principles that would govern digital forensics operations. According to Pollitt [15], the International Association of Computer Investigative Specialists (IACIS) formulated the first set of guidelines for digital forensics. The Association of Chief Police Officers (ACPO) of the United Kingdom also developed the *Good Practice Guide,* which has significantly influenced subsequent developments of digital forensics principles. The International Organization on Computer Evidence (IOCE) and the Group of Eight (G-8) also developed a set of principles for digital evidence. The International High-Tech Crime Conference organised in 1999 adopted specific guidelines to preserve the admissibility of digital evidence [81]. These guidelines and principles are reinforced in the various digital forensics models presented in Section 2.5.

The Council of Europe (CoE) has developed a set of principles relating to digital evidence. The CoE Guide is a derivative of ACPO principles. However, the CoE principles are broad in scope as it has considered other areas, which were not covered by the ACPO Guidelines. For the purpose of the thesis, the CoE guide is further explained to highlight these fundamental principles.

The CoE Guide states five essential principles relating to digital evidence that are represented in Figure 3.1.

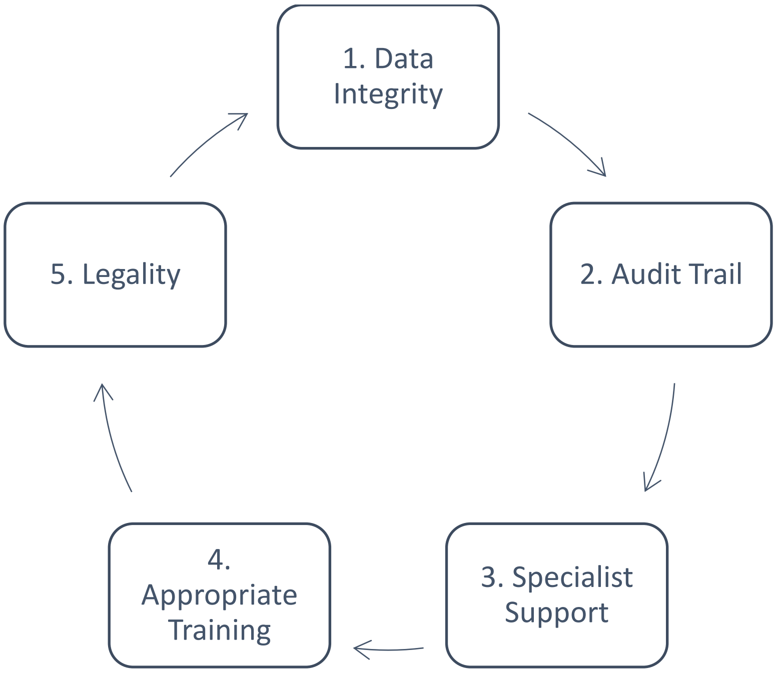


Figure 3.1: CoE Principles of Electronic Evidence [17]

- **Principle 1 — Data Integrity**

No action taken should materially change any data, electronic device or media, which may subsequently be used as evidence in court.

The principle postulates that electronic devices and data must not be changed in the course of investigations, either in relation to hardware or software. Personnel handling the case must assume full responsibility of this core principle, which seeks to protect the integrity of digital evidence.

- **Principle 2 — Audit Trail**

Records of all actions taken when handling electronic evidence should be created and *preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions, but also to achieve the same result.*

The principle explains that it is imperative to record accurately all activities at the crime scene to enable a third party to reconstruct the first responder's actions, if necessary. All activity relating to the search, seizure, access, storage or transfer of electronic evidence must be fully documented and preserved.

- **Principle 3 — Specialist Support**

If it is expected that electronic evidence may be found in the course of a planned operation, the person in charge of the operation should notify specialists/external advisers on time and to arrange their presence if possible.

Due to the highly technical nature of digital evidence and the need for guidance and collaboration, the principle provides advisory for handlers of digital evidence to contact external specialists wherever possible.

- **Principle 4 — Appropriate Training**

First responders must have the necessary and appropriate training to be able to search for and seize electronic evidence if no specialists are available at the scene.

This principle requires handlers of digital evidence, especially first responders to have relevant training and expertise to respond to cyber-related investigations.

- **Principle 5 — Legality**

The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter.

Digital evidence is only acceptable when obtained and applied in appropriate legal contexts. For example, in most jurisdictions a court warrant is required to seize and search electronic devices [3], [67]. This principle mandates officers handling cyber-related investigations to ensure full legal compliance at each stage of the investigations and prosecutions process.

Adherence to the above principles is a pre-requisite for digital evidence to be admitted in a court of law. The principles explained above influenced the development of the various technical and legal requirements of digital evidence admissibility. The next section briefly introduces the concept of digital evidence admissibility and its challenges in legal proceedings.

3.6. Admissibility of Digital Evidence and Admissibility Challenges

Generally, digital evidence is admitted in most jurisdictions, subject to country-specific legal rules of evidence [82]. While global acceptance of digital evidence as a form of evidence marks a significant milestone for the development of digital forensics, specific challenges remain. Digital evidence faces two key hurdles when presented in court. The first is the admissibility of the evidence itself by the court. Before a piece of digital information or data is admitted into evidence, it has to meet certain fundamental requirements. The second hurdle is the determination of evidential weight of the digital information admitted into evidence.

These two difficulties can be understood from both legal and technical perspectives. While the first hurdle is primarily addressed by the law, the second hurdle is often determined by considering a number of technical factors. At this juncture, it is important to present a brief analysis from existing literature on the admissibility of digital evidence as part of the discussions on this subject matter.

The Daubert test [71] remains one of the most important tests of digital evidence admissibility as its influence transcends the United States criminal justice system. The Daubert test revolves around four key factors:

- **Testing:** Can and has the scientific procedure been independently tested?
- **Publication**: Has the scientific procedure been published and subjected to peer review?
- **Error rate:** Is there a known or potential error rate associated with the use of this scientific procedure?
- **Acceptance:** Is the scientific procedure generally accepted by the relevant scientific community?

Considering the existential fragilities of digital evidence and challenges of meeting the criminal burden of proof, the Daubert test has significantly shaped the concept and practice of digital evidence admissibility as it establishes some scientific basis for digital evidence admissibility. Similarly, Federal Rules of Evidence 702 [83] require that scientific and expert testimony must be reliable both with respect to the principles and methods used by the expert and application of the principles and methods to the specific facts.

While the Daubert test sets out the scientific parameters for the admissibility of digital evidence, Daubert neither operationalises the parameters outlined to establish admissibility nor determines the evidential weight of digital information, which is admitted into evidence. Ryan and Shpantzer [84] agree in the sense that even if digital evidence survives the Daubert challenge, it may still face specific technical challenges relative to the collection, storage, processing and presentation of the evidence in question. In addition, the parameters outlined in Daubert effectively address general technical or scientific issues relative to the *scientificity* of a particular forensic methodology. Daubert does not address legal questions of admissibility. Consequently, the Daubert test does not resolve the *techno-legal dilemma* of digital evidence admissibility and evidential weight determination.

The Council of Europe, in its Electronic Evidence Guide identifies specific criteria that form the basis for evaluating digital evidence. These criteria are essential from a legal viewpoint and are therefore presented below:

- **Authenticity:** The evidence must establish facts in a way that cannot be disputed and is representative of its original state.
- **Completeness:** The analysis of, or any opinion based on the evidence must tell the whole story and not be tailored to match a more favourable or desired perspective.
- **Reliability:** There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.
- **Believability:** The evidence must be persuasive as to the facts it represents and the finders of fact in the court process must be able to rely on it as the truth.
- **Proportionality:** The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (i.e., the level of intrusion or coercion) caused to the rights of any party should not outweigh the “probative value” of the evidence (i.e., its value as proof).

While the above are important legal considerations, their practical application in legal proceedings is significantly impacted by technical considerations.

Digital evidence is highly volatile. As earlier argued, digital evidence can rapidly be altered through basic computing-related activities [85]. For example, a basic click of a file on a computer can alter its metadata, which is a key determinant of that evidence's admissibility. Though a user may not necessarily intend to alter the metadata of a file, clicking on it will potentially alter its metadata, such as when the file was last accessed, rendering the file possibly inadmissible. In order to ensure that evidence is admitted, the court must be satisfied that such evidence conforms to established legal rules; the evidence must be scientifically relevant, authentic, reliable and must have been obtained legally [86]. Ryan and Shpantzer [84] support this argument and further explain that digital forensic evidence qualifies to be admissible if only it is deemed relevant to the case and there is proof that the evidence was obtained through the use of a scientific method.

The fragility of digital evidence also presents several challenges [87]. The rapidly-changing nature of technology, the media fragility within which electronic data is stored and the intangible nature of electronic data all render digital evidence potentially vulnerable to claims of errors, accidental alteration, prejudicial interference or fabrication. These technical issues, together with legal missteps or difficulties could affect the admissibility of digital evidence. Even when digital evidence is admitted, such factors could eventually impact the evidential weight of the evidence in question. Indeed, the Federal Rules of Evidence 102 [88] further strengthen the above argument.

Accessing digital evidence often involves securing legal authorisation to do so and failure to do so (secure authorisation) may jeopardise prosecutions. Searches and seizures, if illegally conducted, have serious ramifications that can affect the admissibility of evidence [89]. Criminal justice practitioners acknowledge that this is the first process that is commonly disputed in court cases [64]. If a defendant is able to successfully argue that the procedure for search and seizure was illegal or that there was no probable cause, it can result in a dismissal of the case. Goodison et al. [1] contends that "evidence is of little use to the criminal justice system when it is ruled to be improperly obtained after the fact". Similarly, Brobbey [69] contends that admissibility of evidence in court is dependent on the fact that the piece of evidence is relevant to the fact being proved and that it is procured, processed, preserved and presented in a legally approved manner.

There have been many instances where basic judicial missteps have resulted in the dismissal of cases. For instance, Ami-Narh and Williams [87] provide an example of a criminal case of child pornography where technicians retrieved electronic records from a suspect's email accounts after obtaining a search warrant. Upon presentation of the evidence at a trial, the court ruled that the seizure of the email accounts of the suspect was unlawful due to the absence of police presence, which was a legal requirement. The ruling was however overturned by a higher court. This example nevertheless provides useful lessons on the need to adhere religiously to legal protocols when handling digital evidence. Leigland and Krings [30] further elaborate the technical and legal challenges associated with digital evidence and its application in judicial proceedings.

The challenges associated with digital evidence are the basis of its existential fragility relative to its admissibility and evidential weight determination in legal proceedings. The next section concludes the chapter.

3.7. Conclusion

This chapter introduced the concept and application of digital evidence and presented the foundations of digital evidence and its application in judicial proceedings. The chapter has further established a commonality between digital evidence and other forms of conventional evidence while simultaneously defining the unique characteristics of digital evidence. The chapter also discussed the core principles governing digital evidence and the impact of these principles on the technical and legal requirements of digital evidence admissibility.

Challenges associated with digital evidence admissibility were also discussed extensively by the researcher. The chapter concluded the background discussions with highlights covering the technical and legal bases for digital evidence admissibility. The object of the thesis — determinants of digital evidence admissibility — are presented in the next chapter.

PART 3: INTRODUCTION AND VALIDATION OF THE HARMONISED MODEL FOR DIGITAL EVIDENCE ADMISSIBILITY ASSESSMENT (HM-DEAA)

Part Three of the thesis covers the proposed Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA), a proposed model to resolve the *techno-legal dilemma* relative to digital evidence admissibility. Three chapters are covered under this part — comprising of Chapter 4 to Chapter 6. Chapter 4 discusses the technical and legal determinants of digital evidence admissibility. Chapter 5 introduces the HM-DEAA model by integrating both the technical and legal determinants into an integrated framework, which establishes the foundation of the HM-DEAA. Chapter 6 discusses the survey conducted to validate the model proposed.

CHAPTER 4: DETERMINANTS OF ADMISSIBILITY OF DIGITAL EVIDENCE

4.1. Introduction

From the background review of literature, it has been established that there are specific requirements and factors that underpin the admissibility of digital evidence in judicial proceedings. Furthermore, analysis of the nature of digital evidence and the challenges associated with digital evidence suggest that these requirements and considerations are both technical and legal in nature. This chapter discusses these technical and legal requirements, which are assessed during trials in order to admit a digital record of relevant evidential value into evidence and to determine the evidential weight of the digital material in question.

The word 'determinant' is used in this thesis to refer to the requirements, benchmarks, and/or factors that are considered during judicial proceedings before admitting a particular digital evidence. The determinants are the foundation of the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) model being proposed and they are wholly influenced by the principles of digital evidence, which were presented in Section 3.5.

The researcher has identified a number of these requirements, which are considered technical determinants. These are presented in section 4.2. The remainder of the chapter is constructed as follows: Section 4.3 introduces a number of legal determinants of admissibility of digital evidence. Section 4.4 concludes the chapter with a summary.

4.2. Technical Determinants of Admissibility of Digital Evidence

Digital evidence is produced through a scientific process. There are technical requirements comprising of both activities and processes that underpin the scientific processes through which digital evidence is produced. These determinants are derived from industry standards, scientific research, substantive and procedural legislations, legal precedents and expert opinion, among other sources. The determinants have bearings not only on digital evidence admissibility but also in determining the evidential weight of digital information or records, which are admitted into evidence. Figure 4.1 summarises the specific technical determinants, which constitute the technical foundations of a particular digital evidence. The researcher conducted a survey to validate these determinants. Findings from the survey and detailed analysis are presented in Chapter 6.

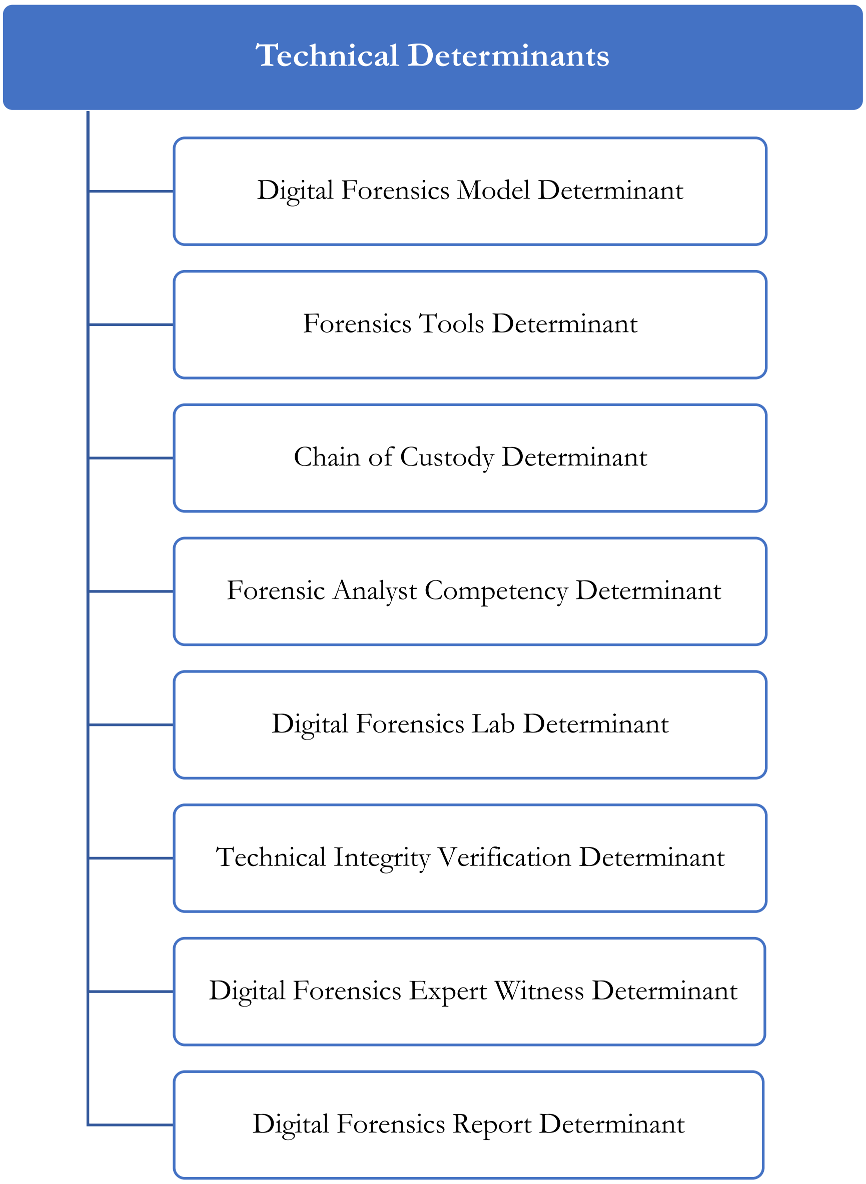

Technical Determinants
Digital Forensics Model Determinant
Forensics Tools Determinant
Chain of Custody Determinant
Forensic Analyst Competency Determinant
Digital Forensics Lab Determinant
Technical Integrity Verification Determinant
Digital Forensics Expert Witness Determinant
Digital Forensics Report Determinant

Figure 4.1: Technical Determinants of Admissibility of Digital Evidence

4.2.1. Digital Forensics Model Determinant

Digital forensic models establish scientific procedures to conduct thorough investigations in order to obtain admissible evidence [12]. These models may be all-inclusive or specific depending on the scope of their application. ISO/IEC 27043 is an example of an all-inclusive forensic model designed for incident investigations. Kalaimannan [90] has introduced a digital forensics procedure for smart devices. This is considered as a specific, target-oriented investigations model. Depending on the target digital environment and the typology of investigations, different approaches are adopted by digital forensic investigators to obtain digital evidence. Each forensic approach or procedure is influenced largely by a number of factors, including the nature of the incident, the type of digital evidence, the typology of the target digital device or the electronic environment. For example, procedures for extracting digital evidence from mobile devices are different from the standard approach for extracting digital evidence from a seized hard drive. Similarly, live forensics require a unique methodology to ensure that evidence produced from such investigative activity is fit for purpose. As a result, the responsibility of the court to assess the admissibility of evidence also includes determining the appropriate forensic approach adopted to retrieve and process the digital evidence in question.

It is important to emphasize that digital forensics as a science does not provide a unique procedure or approach for all typologies of investigations. What digital forensics does is rather to provide universal principles that underpin the various scientific approaches, which have been developed and tested for the various investigation scenarios. Specific guidelines in the form of digital forensic models have been developed to ensure that forensic investigators adopt the appropriate forensics approach in conducting investigations. The ACPO Guidelines [7], the Scientific Working Group on Digital Evidence (SWGDE) Guidelines [33] and ISO/IEC 27043 provide guidelines on digital forensics processes and procedures. For digital evidence to be accepted in a court of law, the model adopted for the investigations should be up to date [12].The court is duty bound to demand that the right digital forensic approach was adopted in the production of a particular evidence that is introduced at a trial.

4.2.2. Digital Forensics Tool Determinant

Digital forensic practitioners have access to a variety of both open source and proprietary tools to assist the analysis and preservation of digital evidence. The appropriate digital forensics tools are required to search, locate and preserve digital evidence. Even though there are no explicit rules governing the use of digital forensic tools, there is a general consensus within the scientific community that forensic tools should have been tested, validated and their known error rates documented [71]. These guidelines are very important, partly because of the fragility of digital evidence and its inherent vulnerability to manipulation by accident or malicious actions. The Daubert test further highlights the importance of digital forensics tools validation as a criterion in determining the admissibility of digital evidence [71]. Different bodies have been active in providing frameworks and methods for the testing of digital forensic tools. These include the National Institute of Standards and Technology (NIST) in the United States, the Scientific Working Group on Digital Evidence (SWGDE) and the International Organization for Standardization (ISO), ISO/IEC 27041 [91]. The court has a responsibility to ascertain that the forensic tool used to process a particular digital evidence is scientifically tested with its accuracy and reliability known.

4.2.3. Chain of Custody Determinant

Chain of custody refers to processes involved in preserving the integrity of digital evidence. The United States National Institute of Justice defines chain of custody as a process used to maintain and document the sequential history of evidence [92]. Chain of custody documentation cuts across all steps of the investigative process and is particularly important at the digital evidence seizure stage. Chain of custody applies to incident discovery, documentation of digital exhibits, transportation of digital exhibits, forensic acquisition and processing of digital artefacts, and preservation of digital evidence. Chain of custody starts the moment that an incident is discovered, or a case is lodged, whatever the case may be. Crime scene documentation is an important component of chain of custody documentation.

The unique characteristics of digital evidence, including its inherent fragility makes chain of custody in digital forensics an indispensable requirement for digital evidence admissibility. According to one of the principles of digital forensics as outlined in the ACPO Guidelines, an independent third party should be able to track the movement of the evidence right from the crime scene along the investigations chain to the court room [7]. According to Giova [93], digital evidence should be accepted as valid in court only if the evidence's chain of custody can be established.

4.2.4. Forensic Analyst Competency Determinant

Qualification of a digital forensic analyst or examiner is another important determinant pertaining to digital evidence admissibility in judicial proceedings. As presented in Chapter 2, digital forensics as a forensic science is a multidimensional discipline that encompasses computing (information technology), investigations and law. The digital forensics examiner is expected to demonstrate his/her "digital forensics competency" in order to handle digital evidence. Even though no transnational competency standards have been developed to validate the forensic competency of a digital forensics examiner, previous background education and experience, digital forensics certification and hands-on industry experience in digital forensics are normally considered to determine the suitability of a person to handle digital evidence.

In assessing digital evidence admissibility and the basis of attributing evidential weight to a digital evidence, the courts are usually required to ascertain the qualifications of the forensic analyst or expert pertaining to the evidence. It is not enough for the digital forensics analyst to retrieve digital evidence from a target digital device or environment. But as one of the important principles of digital evidence requires, s/he should be able to explain the relevance of the forensic techniques and approaches adopted to produce the evidence. Knowledge, experience and professional competence of a forensic examiner or digital forensics investigator could significantly impact not only his/her ability to forensically process digital evidence, but also his/her ability to provide scientific interpretation of digital evidence.

4.2.5. Digital Forensics Lab Determinant

It is a common opinion within the digital forensic community that well-organised digital forensics labs with standard operating procedures (SOPs) and quality assurance systems impacts the quality and productivity of investigations processes and, consequently, the quality of evidence produced from such a facility. The use of a poor laboratory facility or inappropriate storage procedures could result in digital evidence being refused at a trial [94].

The American Society of Crime Laboratory Directors (ASCLD) [95] and the ACPO Good Practice Guide [7] provide specific professional guidelines for setting up and operating a digital forensics lab. For example, a digital forensics lab should be accessible only to authorised forensic examiners and personnel only because of chain of custody and other requirements. As a result, a digital forensics lab should have adequate access control mechanisms in order to ensure the integrity of evidence.

There are other examples that highlight the impact of the forensics lab on digital evidence. For instance, cell phones are required to be isolated and normally kept in Faraday bag[4] upon seizure in order to prevent remote modification, locking or wiping. Failure to adopt the above practice as a laboratory standard operating procedure could alter the current state of data stored on a mobile device. Most jurisdictions require seized devices and equipment to be stored in a secured laboratory as a chain of custody determinant.

4.2.6. Technical Integrity Verification Determinant

Maintaining and verifying the integrity of a digital evidence object is an important technical consideration that could impact significantly on legal considerations for the admissibility of digital evidence. Digital data can easily be altered, modified or copied from one environment to the other through human actions and uncontrolled computing activities [85]. Forensic examiners are required to adopt specific evidence validation methods and safeguards to ensure integrity of digital evidence.

Different methods of maintaining and demonstrating integrity of digital evidence are normally adopted by forensic examiners. The use of write blockers, for example, is a standard digital forensics requirement to maintain integrity of evidence. The use of digital signatures, encryption and relevant hash algorithms are also employed to maintain, validate and demonstrate integrity of digital evidence. In addition, chain of

[4] Faraday bag is an enclosure to shield electromagnetic fields. Faraday bags are usually used by investigators in the collection, preservation, transportation, and analysis of cellphones and other wireless devices. Wireless devices such as cell phones and bluetooth enabled devices are shielded from cellular, wireless and other radio signals by the Faraday bags. This prevents potential tampering of digital evidence. The name Faraday is linked to Michael Faraday, a British electromagnetic scientist. http://faradaybag.com/2018/01/.

custody documentation validates the integrity of the forensic procedures adopted from the start of the investigations until a final report covering the case is submitted.

4.2.7. Digital Forensics Expert Witness Determinant

The variety of domains in digital forensics and emerging complexities in the field requires expertise to support judges in determining cases involving digital evidence [96]. The use of expert witness in the court of law is practised in most jurisdictions. Digital forensics is one of several specialty areas for which a court may (and often does) employ the opinion or testimonies of an expert. This is partly because the field is relatively new and traditional stakeholders within the criminal justice system like judges, defence lawyers, law enforcement investigators and prosecutors have limited knowledge and understanding of the technical matters pertaining to digital evidence. To arrive at best judgement, a court will often call on individuals with the relevant expertise, knowledge and skill in a particular area to serve as witnesses during trials [97]. For a person to serve as an expert witness, the Federal Rules of Evidence in the United States require that such a witness must be qualified by knowledge, expertise, experience, education or training. His/her scientific, technical or any specialized knowledge must be capable of assisting in determining the fact in use [97]. As a result, a digital forensics expert witness ought to be deemed an expert, vested in the knowledge and practice of digital forensics. The Daubert standard also highlights the relevance of the qualification of an expert witness to testify in court as an expert witness.

Schroeder [97] makes an important argument and explains that when a digital forensic expert is called upon to testify before a court over a cyber incident or a digital evidence, such an expert is assuming a dual role. The first role requires that the testimony to the court should be factual. For example, the expert witness provides answers to questions regarding the fact of the matter as presented to the court. The additional role occurs when the expert provides his/her opinion, which reflects his/her expertise, experience and knowledge in the field. It is important to emphasize that reliance on expert witnesses is not adequate if the court cannot discern that the opinion presented by the expert is accurate and factual [98]. This situation typically occurs in jurisdictions where the active players within the criminal justice system are not well informed about digital forensics and digital evidence

4.2.8. Digital Forensics Report Determinant

The digital forensics report is an important technical consideration that underpins digital evidence admissibility in a court of law. The role of the forensic examiner is very crucial in establishing the authenticity and reliability of digital evidence as the merit of a case virtually rests on him/her. Upon the completion of forensic examination, the examiner is required to produce a report that captures the details of findings of his/her examination of the evidence. An omission of any factual detail or addition of erroneous information whether wilful or accidental could have serious ramifications on the evidence. In certain jurisdictions, deliberately withholding relevant information from a forensic report could in itself constitute criminal conduct and result in legal action against the forensic examiner or the expert.

Garrie and Morrissy [99] have postulated that the forensic report must have conclusions that are reproducible by independent third parties. This means that a forensic report must document all steps taken by the examiner with sufficient details so that an independent third-party can replicate the conclusions. A digital forensics report must document all discovered facts and all formed opinions with traceable sources. In *Republic vs. Alexander Tweneboah* [100], the high court judge at the financial court division ruled against a report submitted by an expert witness from the e-Crime Bureau because, according to the judge, the report did not fully represent the digital evidence contained on an accompanying CD. Garrie and Morrissy [99] explain that reports with conclusions that are not reproducible should be granted little credence in a court of law.

This chapter has identified and discussed the various technical determinants of digital evidence admissibility in legal proceedings. The relevance of these technical determinants in legal proceedings has been established. The next section discusses the various legal determinants and how they impact digital evidence admissibility in criminal prosecutions.

4.3. Legal Determinants of Admissibility of Digital Evidence

ln every jurisdiction, there are legal requirements that govern the grounds for the admissibility of digital evidence. These requirements are well-grounded in legal philosophy and case law and constitute the legal determinants of digital evidence admissibility. These legal determinants have their origins in substantive and procedural legislations, legal precedents and other legal arrangements of a particular jurisdiction. Increasingly, international conventions such as the Budapest Convention on cybercrimes [62] provide legal basis for the admissibility of digital evidence. This section presents the legal narrative regarding the admissibility of digital evidence as summarised in Figure 4.2.

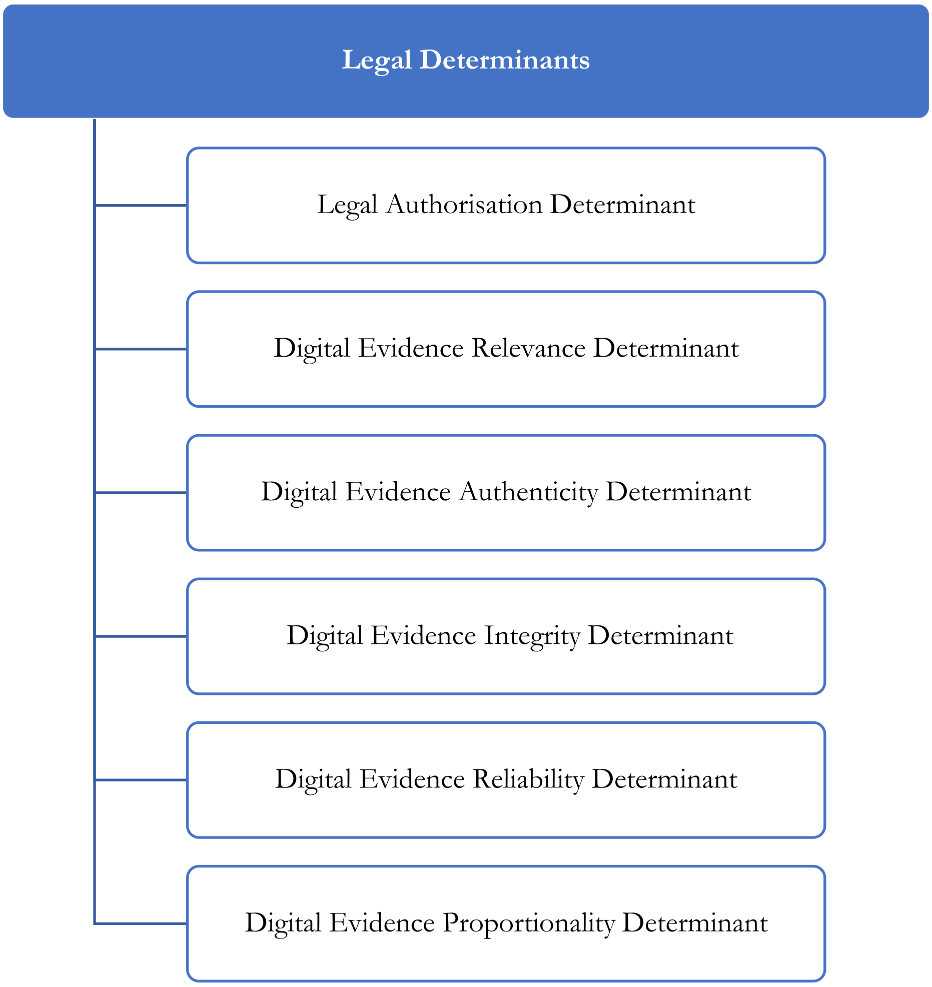

Legal Determinants
Legal Authorisation Determinant
Digital Evidence Relevance Determinant
Digital Evidence Authenticity Determinant
Digital Evidence Integrity Determinant
Digital Evidence Reliability Determinant
Digital Evidence Proportionality Determinant

Figure 4.2: Legal Determinants of Admissibility of Digital Evidence

4.3.1. Legal Authorisation Determinant

Assessing digital evidence often involves securing legal authorisation to do so. Human rights, data protection and privacy issues are fundamental rights of individuals, including criminal suspects that need to be respected. This is because a criminal suspect is not a convict until a competent court pronounces a judgement of conviction. In addition, most criminal legislations provide safeguards concerning the rights of suspects. Even though there could be exceptions, the law generally provides safeguards for the protection of individuals' rights. Obtaining legal authorisation grants judicial legitimacy for the evidence in question and this is considered the most important first step in obtaining and handling digital evidence. Search warrants are normally used to obtain electronic devices or digital evidence. A court normally grants authorisation through a warrant for a specific information or electronic data. Failure to obtain legal authorisation may undermine the best evidence rule and could jeopardise prosecutions [86].

Digital forensics searches and seizures, if proven to be illegally conducted, could have serious consequences that can affect the admissibility of evidence [89]. In many jurisdictions, the process of undertaking search and seizures presents several vulnerabilities that could potentially undermine the integrity of the prosecutions. In the United States, evidence acquired illegally is termed "Fruit of the Poisonous Tree " and is generally inadmissible in court [85]. In other jurisdictions, including in South Africa, the court may use its discretion to either admit or refuse digital evidence presented under such circumstances. In some countries, including Israel, such evidence may be admitted but shall receive less evidentiary weight [85], [82]. Admitting evidence not backed by any legal authorisation could result in law enforcement and the state trampling on the liberties of citizens [69]. In the United States, the Privacy Protection Act (PPA) limits the abuse or misuse of search warrants to search for or seize electronic devices. In all legal jurisdictions, the rule of law underpins the legal authorisation determinant for obtaining digital evidence.

4.3.2. Digital Evidence Relevance Determinant

Relevance is an important determinant for the admissibility of digital evidence. According to Mason [82], in order for evidence to be admissible, it must be "sufficiently relevant" to the facts in issue. Evidence cannot be admissible if it is not deemed to be 'relevant' [86]. Thus, for the evidence to be relevant it must be capable and directed at proving or disproving a case under prosecutions. According to Brobbey [69], evidence is relevant if it is logically probative or disprobative of some matter that requires proof. For any piece of evidence to be considered relevant in a court of law, the evidence in question must tend to prove or disprove a fact in a case under trial or prosecutions. Evidence with probative value must have the ability to prove the fact to be more probable than it would be without the evidence.

Under Section 55 of the Uniform Evidence Act of Australia, evidence is considered relevant if it is capable of rationally affecting the assessment of the probability of a fact and issue in legal proceedings [82]. In most common law jurisdictions such as the United Kingdom and Canada, for evidence to be admissible, it must be relevant to a fact that is material [82]. As a general rule, evidence can only be admissible if it is deemed to be "relevant" [16]. In most jurisdictions, obtaining digital evidence without a probable cause can result in a dismissal of the case.

4.3.3. Digital Evidence Authenticity Determinant

Authenticity is another important criterion that impacts on the reliability of evidence. According to Mason [82], for digital evidence to be admitted in a court of law, there must be evidence adduced that the document is what it is purported to be. For example, for digital record to be admissible, the court will have to be convinced that the document or the record was generated by the author who is accused to have generated it. Authentication means satisfying the court that the contents of the record have remained unchanged and that the information in the record originates from its purported source whether human or machine. Authentication also means that metadata or properties associated with evidence files are accurate. Technically, hash values are also used to authenticate electronic records.

In most jurisdictions, court rules require that evidence must be authenticated before it is admissible. Such evidence must be what a proponent claims it is. This implies that the evidence is a true and accurate representation of what the evidence is claimed to be. In order to establish authenticity of electronic records, external parties such as a system administrator can testify that log files associated with a web server presented in court originated from a particular system or server. Authenticity of digital evidence is usually challenged in court. Apart from establishing the technical procedures adopted to obtain the evidence, the availability of technical or expert witness to the courts help to address issues arising from digital evidence authenticity.

A typical case example, which highlights the relevance of the authenticity determinant, is the case of *American Express Travel Related Services Company Inc., vs. Vee Vinhnee.* The trial judge argued that American Express failed to authenticate certain records in digital format and therefore the case was ruled against American Express on the basis of its failure to authenticate the records. Subsequently, American Express appealed against the decision, but the earlier decision of the trial judge was affirmed [82].

4.3.4. Digital Evidence Integrity Determinant

The availability of relevant evidence does not merely imply that there will be successful prosecution or that the evidence will be admitted in court. Evidence integrity refers to the 'wholeness and soundness' of digital evidence [82]. Integrity refers to the evidence being complete and unaltered. Evidence integrity determinant is a primary determinant of admissibility of digital evidence and the basis for determining the evidential weight. Using evidence integrity assessment, the court normally determines the due processes followed right from collection of evidence, to its storage and presentation. Digital evidence integrity refers to the fact that the evidence presented is whole and unaltered from the time of acquisition until its presentation to the court.

Mason [82] contends that digital evidence integrity is not an absolute condition but rather a state of relationships. In assessing the integrity of digital evidence, the courts therefore consider several factors and relationships primarily the technical determinants presented in the previous section. The courts require integrity of evidence to be established and guaranteed during investigations and to be preserved from any modifications during the entire life cycle of the evidence as relevant to the court [86]. In South Africa, the originality of digital evidence depends on its integrity, as outlined in Section 14 (2) of the Electronic Communications and Transactions (ECT) Act of 2002. Section 17 of the ECT Act of 2002 provides guidelines for judging the integrity of digital evidence.

4.3.5. Digital Evidence Reliability Determinant

Reliability of digital evidence is another consideration in a court of law to determine digital evidence admissibility and to establish the evidentiary weight of evidence admitted. This determinant is directly linked to a number of technical determinants underpinning evidence admissibility. In order for evidence to be admissible in court, the prosecutor must be able to and actually establish that no aspect of the evidence is doubtful. According to Zhao [101] digital evidence has been questioned in the courts because of reliability issues. The reliability of any piece of evidence is normally challenged during judicial proceedings, either through cross-examination or by the opposing party's expert. Flaws in scientific procedures and methods such as adopting inappropriate digital forensics model could raise reliability issues [102]. Leroux [86] explains that for evidence to be deemed reliable "there must be nothing that casts doubt about how the evidence was collected and subsequently handled". Generally, reliability of evidence is also determined by a number of scientific (technical) factors. For evidence to be reliable, it must be authentic, accurate and complete.

In the United States, the *Daubert* test provides the basis for assessing reliability of scientific evidence such as digital evidence. In determining the admissibility of digital evidence, the *Daubert* standard outlines five criteria: whether the technique has been tested; whether the technique has undergone peer review; whether there is a known error rate associated with the technique; the existence and maintenance of standards controlling its operations, and whether the technique is generally accepted by the scientific community [71]. These criteria presuppose technical considerations that consequently impact the reliability of evidence as a legal criterion.

In South Africa (S v Singh and Another), a judge refused to admit a tape recording as evidence because the prosecution succeeded in convincing the court that the evidence that the prosecution was relying on had been interfered with [82]. Errors in the digital forensics process could affect the reliability of digital evidence. Reliability as a judicial criterion for assessing admissibility of evidence is highly dependent on technical determinants pertaining to digital evidence. According to Goodison et al. [1], new advances in technology and forensic techniques will continue to raise issues bordering on reliability.

4.3.6. Digital Evidence Proportionality Determinant

Proportionality as a legal concept has its root in ancient judicial philosophy of justice [103]. The principle of proportionality, which is a liberal legal doctrine, requires that any interference with rights such as the rights of a suspect should not be disproportionate relative to the interest of the investigations. This implies that even after legal authorisation has been granted for the commencement of digital forensics activity, subsequent actions of parties involved including forensic examiners should not be significantly disproportionate. According to Mason [82], some jurisdictions have introduced proportionality rules into their legal rules because of privacy and civil liberty concerns. In some jurisdictions, judges have used their discretionary powers to decline production orders that appear oppressive or excessive in scope. In the English legal system, judges make disclosure request decisions based on a number of factors including reasonableness, relevance and proportionality [82].

One area of application of the proportionality determinant is the examination of suspect devices. The proportionality determinant obliges the digital forensics investigator to obtain only the information or electronic data that the law has authorised to be accessed. For example, the proportionality requirement prevents the investigator from accessing every information or data on a hard drive when a search warrant authorises the investigator to find specific information in connection with the case. Though the investigator may seize the entire hard drive, s/he is obliged to look for specific information which has been authorised by law through the search warrant. The proportionality consideration is very important in safeguarding human rights and civil liberties.

4.4. Conclusion

This chapter has discussed the specific technical and legal determinants, which impact on digital evidence admissibility. As is already been argued in Chapter 3, these determinants are underpinned by the key principles of digital evidence, which is presented in Section 3.5. The integration of these technical and legal determinants provide the foundation for a harmonised framework to assess digital evidence admissibility. It is important to underline that cross examination as a practice in judicial proceedings is an important element that helps with the assessment of both the technical and the legal determinants which are presented in the chapter. Resolving the *techno-legal dilemma,* which is the foundation of the thesis, implies integrating these two determinants into an operable framework. The next chapter of the thesis discusses the relationship between these determinants in resolving this dilemma.

CHAPTER 5: MODEL FOR DIGITAL EVIDENCE ADMISSIBILITY ASSESSMENT

5.1. Introduction

A judge's decision to admit digital evidence at a trial is dependent on a number of both technical and legal determinants, which have been presented in the previous chapter. The techno-legal foundation of a piece of evidence is what establishes a case's legitimacy at a trial. This chapter presents the integration of both the technical and legal determinants into an integrated framework that provides the foundation to assess digital evidence in criminal proceedings.

The remainder of the chapter is constructed as follows: Section 5.2 discusses the need for the harmonisation of both technical and legal determinants to establish the admissibility of digital evidence. Section 5.3 discusses the framework underlying the proposed digital evidence admissibility assessment model. The researcher presents the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) in section 5.4. Section 5.5 concludes this chapter with a summary.

5.2. Towards Harmonisation of Technical and Legal Determinants

Analysis of literature suggests that existing research, guidelines and standards on digital forensics have not addressed the question of digital evidence admissibility from a holistic perspective. While existing frameworks and standards provide technical processes and guidelines for the incident investigator to follow in conducting digital investigations toward obtaining digital evidence, factors that underpin the admissibility of digital evidence have not been holistically addressed by available standardisation models. The application of digital forensics in judicial proceedings is arguably the most significant relevance of digital forensics as a forensic science. Consequently, there is the need for an integrated framework comprising technical and legal determinants to provide criminal justice actors the basis for determining the admissibility of digital evidence.

Chapter 4 has established that both technical and legal determinants impact digital evidence admissibility in legal proceedings. The interactions between these determinants then determine, whether a piece of evidence is admissible and secondly, the evidential weight of the evidence admitted. In most jurisdictions, a legal authorisation or search warrant (legal determinant) is required before any digital device can be seized for digital forensics examination (technical determinant). Equally, the manner in which electronic evidence is retrieved during forensic analysis (technical determinant) impacts on the reliability of the evidence (legal determinant).

As a result, the harmonisation of both technical and legal determinants constitutes the foundation of digital evidence admissibility determination during criminal proceedings. Figure 5.1 highlights an integrated representation of both the technical and legal determinants, which underpin digital evidence admissibility.

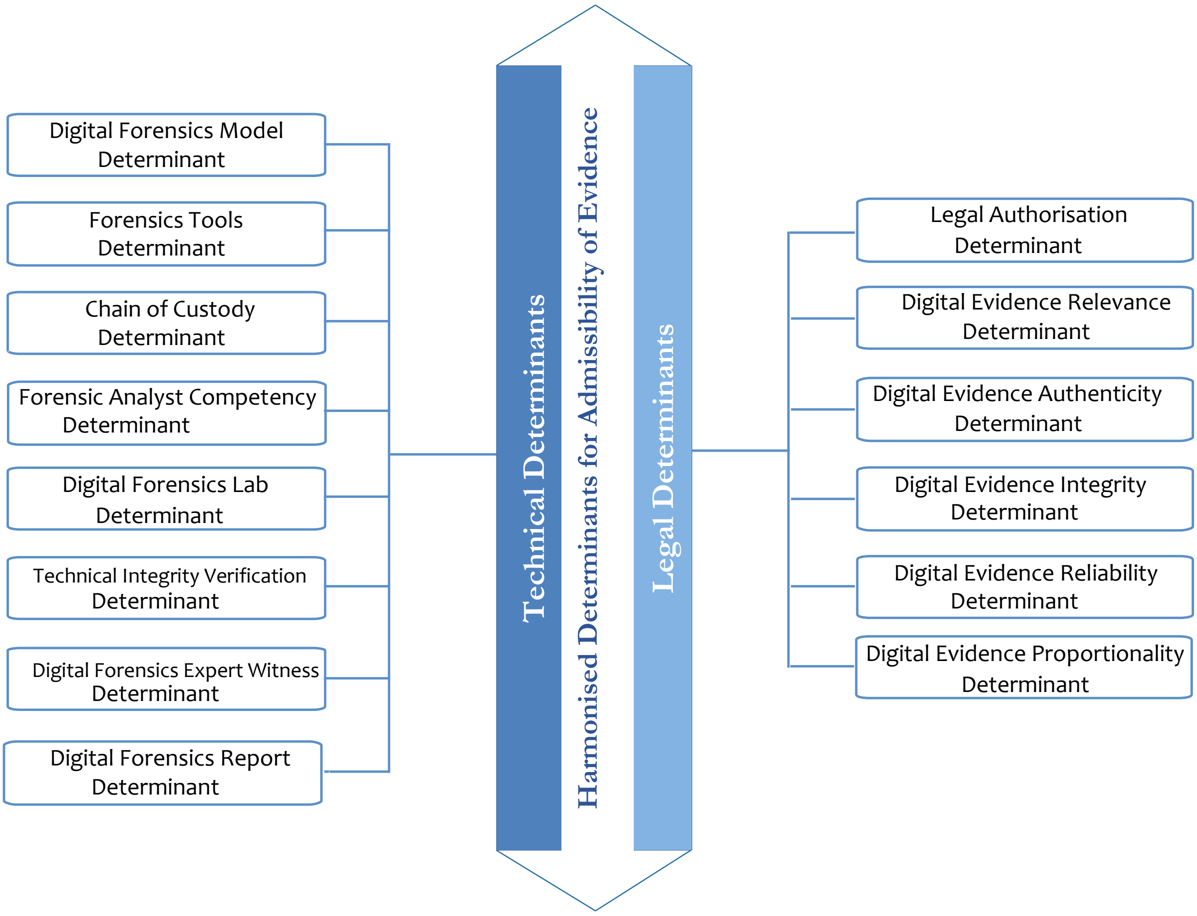

Digital Forensics Model Determinant
Forensics Tools Determinant
Chain of Custody Determinant
Forensic Analyst Competency Determinant
Digital Forensics Lab Determinant
Technical Integrity Verification Determinant
Digital Forensics Expert Witness Determinant
Digital Forensics Report Determinant
Technical Determinants
Harmonised Determinants for Admissibility of Evidence
Legal Determinants
Legal Authorisation Determinant
Digital Evidence Relevance Determinant
Digital Evidence Authenticity Determinant
Digital Evidence Integrity Determinant
Digital Evidence Reliability Determinant
Digital Evidence Proportionality Determinant

Figure 5.1: Technical and Legal Determinants of Admissibility of Digital Evidence

The integration of the determinants shown in Figure 5.1 is discussed further in the next two sections.

5.3. Framework for Digital Evidence Admissibility Assessment

This section discusses the proposed *Harmonised Model for Digital Evidence Admissibility Assessment* (HM-DEAA) and its application in judicial proceedings. The researcher has introduced this model, which is based on the fundamental technical and legal determinants to resolve the *techno-legal dilemma,* which has been introduced as the central theme in this research.

In order to integrate the above determinants, the researcher has developed a harmonised conceptual model, which provides the framework to establish the dependencies and relationships between the various determinant considerations as shown in Figure 5.2.

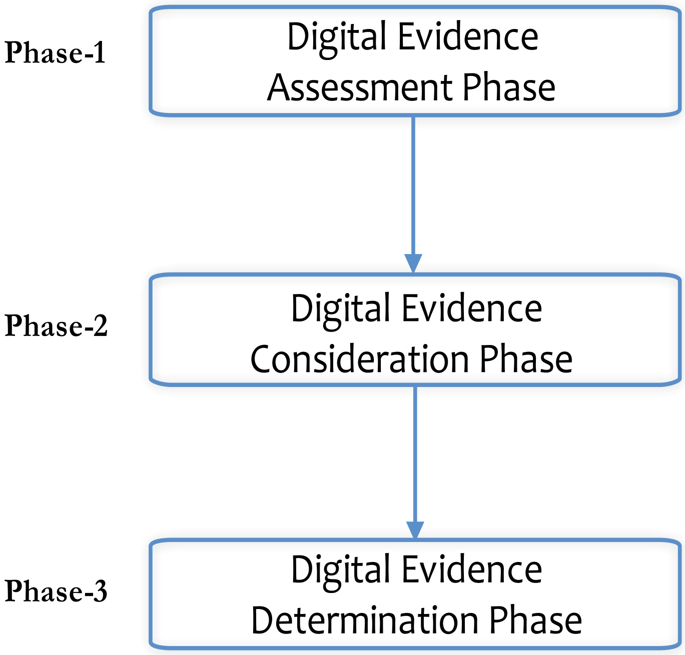

Phase-1
Digital Evidence Assessment Phase
Phase-2
Digital Evidence Consideration Phase
Phase-3
Digital Evidence Determination Phase

Figure 5.2: Model for Digital Evidence Admissibility Assessment Schema

The introduction of the above conceptual framework is borne out of the fact that, the integration of legal and technical determinants is an interactive process with significant dependencies. In other words, the process of establishing digital evidence admissibility is a continuous interactive one involving the various determinants. This interaction is essential to resolving the technical and legal challenges associated with digital evidence and its admissibility in the courts.

The above conceptual model encapsulates three levels of harmonisation called phases, which have been integrated into the proposed HM-DEAA. The three phases are integrated yet distinctive from each other based on their functional relevance in digital evidence admissibility assessment during trials. It is important to highlight that although the phases are integrated based on the conceptual model presented above, each phase is unique due to its functional role in addressing the *techno-legal dilemma.* The next section discusses the HM-DEAA model and its theoretical application to digital evidence admissibility assessment.

5.4. Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA)

The proposed HM-DEAA is designed to rationalise and standardise digital evidence admissibility during criminal trials. The HM-DEAA model is represented diagrammatically in Figure 5.3.

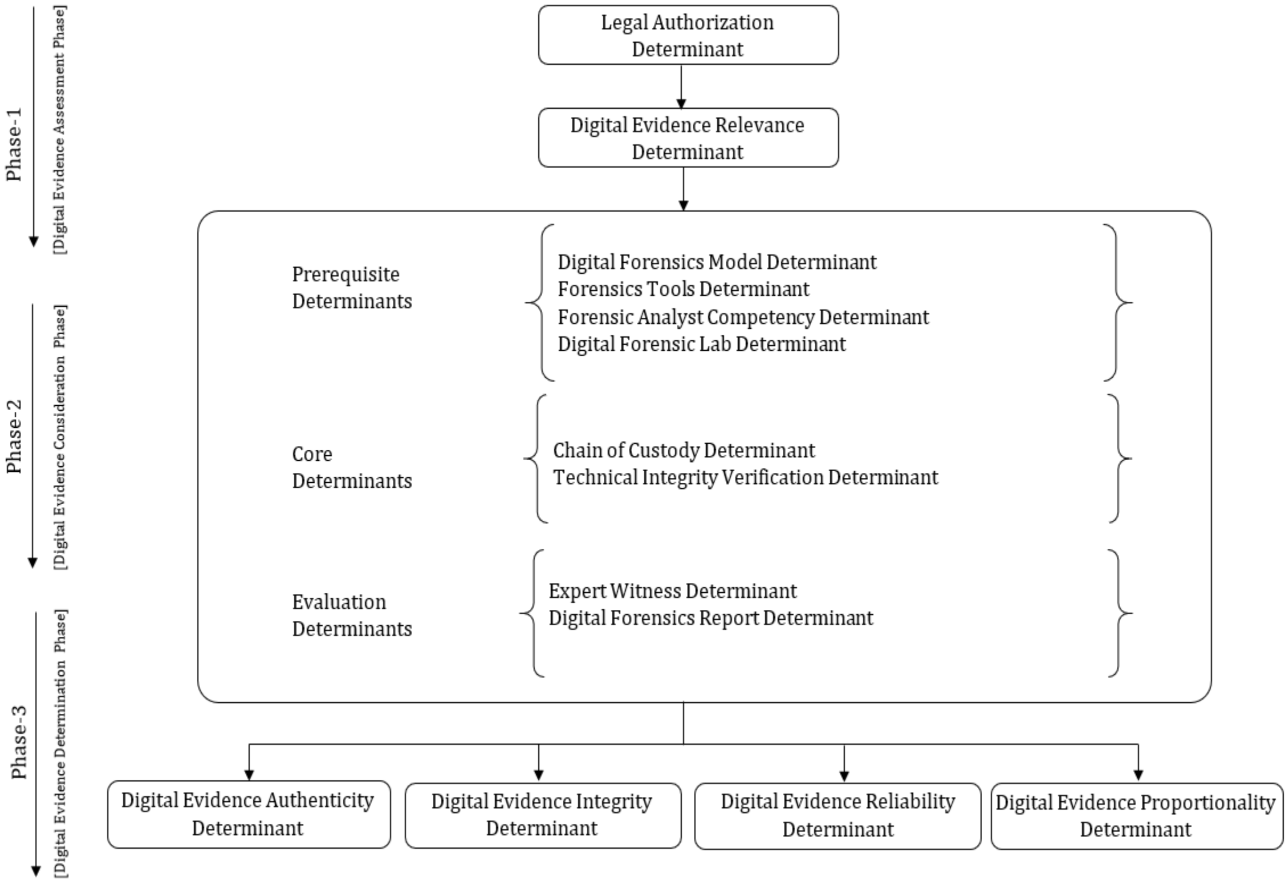

Phase-1
[Digital Evidence Assessment Phase]
Phase-2
[Digital Evidence Consideration Phase]
Phase-3
[Digital Evidence Determination Phase]
Legal Authorization Determinant
Digital Evidence Relevance Determinant
Prerequisite Determinants
Digital Forensics Model Determinant
Forensics Tools Determinant
Forensic Analyst Competency Determinant
Digital Forensic Lab Determinant
Core Determinants
Chain of Custody Determinant
Technical Integrity Verification Determinant
Evaluation Determinants
Expert Witness Determinant
Digital Forensics Report Determinant
Digital Evidence Authenticity Determinant
Digital Evidence Integrity Determinant
Digital Evidence Reliability Determinant
Digital Evidence Proportionality Determinant

Figure 5.3: Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA).

The three phases that underpin the HM-DEAA, are discussed in the sections that follow.

5.4.1. Phase 1: Digital Evidence Assessment Phase

The *Digital Evidence Assessment* phase specifically establishes the legal foundations of the digital evidence in question. For example, when digital evidence (such as a hard drive) belonging to a suspect is presented in court, the court's first consideration is to determine the legal basis for the seizure of the hard drive. Essentially, what this means is that the legal authority of the prosecution that seized and searched the device has to be firmly established. In most jurisdictions, a court order may satisfy this requirement. There are specific cases when exception rules apply, which mandates law enforcement officials to seize digital devices without a court order or a warrant. For example, under Ghana's criminal laws police officers are professionally and legally bound to arrest and seize digital devices when there is reasonable ground or suspicion that a crime is being committed[5]. Organisational policies and protocols also provide the basis for this legal authority. Phase 1, therefore addresses the preliminary questions bordering on legal admissibility of digital evidence. On the whole, digital evidence is deemed inadmissible if it fails to meet the requirements of this important phase. This phase provides the grounds for further consideration of the digital evidence in question as described in the next section.

5.4.2. Phase 2: Digital Evidence Consideration Phase

This phase constitutes scientific and technical industry standards and requirements that underpin digital evidence admissibility. Technical determinants associated with the handling and processing of digital evidence is considered after the legal basis of the evidence has been established in Phase 1. This phase is functionally sub-divided into three categories:

[5] The above mandate is captured under Ghana's Criminal Act, 1960 (Act 30) [122].

1. *Prerequisite Determinants*: These are determinants that need to be considered before any of the core technical activities are conducted. These include the digital forensics model determinant, the forensic tools determinant, the forensic analyst competency determinant and the digital forensics lab determinant. These determinants require certain initial or preparatory activities and processes to be completed as part of a particular digital forensics activity, hence the name “prerequisite”. In the corporate environment, digital forensics readiness can be considered a pre-requisite state or consideration for effective investigations response in case of cyber incidents.

2. *Core Determinants*: These are the main technical determinants that significantly impact on the determination of any digital evidence in question. These determinants make up a chain of custody and technical integrity verification determinants.

3. *Evaluation Determinants:* These constitute considerations that further elaborate or explain the determinants in the previous categories — both prerequisite and core determinants. These include expert witness and digital forensics report determinants.

The above phase, which focuses on technical determinants and considerations of digital evidence, is very important because judicial conclusions (Phase 3) are based primarily on the assessment outcomes of technical determinants. The next phase elaborates on these determinants, which form the basis for judicial conclusions pertaining to digital evidence.

5.4.3. Phase 3: Digital Evidence Determination Phase

This phase underpins judicial decisions by the court in determining the admissibility and evidential weight of digital evidence. Determination of each of the Phase 3 determinants is based on evaluation outcomes of Phase 2 determinants (technical determinants). Determination of the evidentiary weight of a piece of digital evidence is based on findings from the various technical determinants and each of the technical determinants has a specific impact (impact factor) on the evidence. For example, as already highlighted in the previous chapter, even though lack of a digital forensics lab may impact on the outcome of a case involving digital evidence, failure to document and track the chain of custody of an exhibit or piece of digital evidence could have a wider impact on the evidence than the former, as this could significantly affect the evidential weight of digital evidence associated with a case before a court of law. The issue of evidential weight of a piece of digital evidence is addressed further in Chapter 7.

5.5. Conclusion

The researcher has proposed a harmonised model, which provides a holistic techno-legal foundation to assess digital evidence admissibility in a court of law. The model integrates key technical and legal determinants, which underpin evidence admissibility across different jurisdictions. The HM-DEAA provides a framework to operationalise digital evidence assessment and determination of evidential weight of digital information admitted into a trial, which the researcher covers in the next chapters of the thesis.

The HM-DEAA model has established an integrated foundation by which a court can determine the admissibility of digital evidence. The framework presented essentially presents judges with a tool to aid the process of admitting evidence into a trial as well as ascertaining the strength of evidence admitted through a scientific evaluation of each of the determinants considered. Such scientific evaluation is expected to support sound judicial decisions on cases handled by courts.

To further strengthen the scientific basis for the model introduced, the research conducted a validation survey. The ensuing chapter presents findings from a survey and analysis underlying the validation of the HM-DEAA framework.

CHAPTER 6: SURVEY ON DETERMINANTS FOR THE ADMISSIBILITY OF DIGITAL EVIDENCE

6.1. Introduction

The determinants presented in Chapter 4 were derived from industry standards, scientific research and case laws from a number of jurisdictions and expert opinions among other sources. The researcher conducted a survey to validate the identification, categorization and relevance of these determinants in establishing the foundations of digital evidence in practice. The need for the survey was also grounded in the fact that responses from survey participants provided the basis for further development in the operationalization of the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) through evidential weight determination, which is presented later in Chapter 7.

The remainder of this chapter is constructed as follows. Section 6.2 discusses the objectives underlying the survey as well as the design adopted for survey. Section 6.3 examines the survey methodology in the form of survey sampling and data collection. Section 6.4 discusses findings from the survey and their implications for the research. Section 6.5 concludes the chapter with a summary.

6.2. Survey Objectives and Design

The survey conducted was underpinned by the following objectives:

1. Validate the various technical determinants for the admissibility of digital evidence.
2. Identify any other technical determinants (not yet identified) that impacts the admissibility of digital evidence.

3. Determine the impact of each of the technical determinants on the evidential weight of a piece of digital evidence.
4. Validate the various legal determinants for the admissibility of digital evidence.
5. Identify any other legal determinants (not yet identified) that impacts the admissibility of digital evidence.
6. Determine the impact of each of the legal determinants on the evidential weight of a piece of digital evidence.

A questionnaire was administered to survey participants, as shown in Appendix C, after ethical clearance was obtained from the University of Pretoria, as shown in Appendix D. Respondents were asked to indicate whether the various determinants affect the admissibility of digital evidence. Table 6.1 highlights the various determinants and their corresponding abbreviations that are used in later discussions and figures.

Table 6.1: Determinants of Admissibility of Digital Evidence and their Corresponding Abbreviations

S/N	Determinant	Abbreviated Form
1.	Digital Forensics Model	DFM
2.	Forensic Tools	FT
3.	Chain of Custody	CoC
4.	Forensic Analyst Competency	FAC
5.	Digital Forensics Lab	DFL
6.	Technical Integrity Verification	TIV
7.	Digital Forensics Expert Witness	DFEW
8.	Digital Forensics Report	DFR
9.	Legal Authorisation	LA
10.	Digital Evidence Relevance	DERe
11.	Digital Evidence Authenticity	DEA
12.	Digital Evidence Integrity	DEI
13.	Digital Evidence Reliability	DERl
14.	Digital Evidence Proportionality	DEP

6.3. Survey Methodology, Sampling and Data Collection

The researcher adopted an integrated mixed method, a research method that combines both quantitative and qualitative approaches. This method is particularly recommended in research [104] because it incorporates the strengths of both qualitative and quantitative approaches. Beside, being scientifically ideal to address the research objectives above (Section 6.2), this approach also helped to reduce the weaknesses of each of the methods [104] and enhanced their respective methodical strengths.

The qualitative method used comprised a survey of a target sample population. The qualitative metrics were represented by a Likert scale. Likert scale is a psychometric response scale, which is used in research that employ questionnaires to obtain participant's preferences or degree of agreement with a statement or set of statements [105]. The survey was conducted primarily to validate the identified determinants. Any weaknesses arising from the qualitative data collection were addressed through a redundancy test as all respondents were administered the same survey questionnaire, which was approved by the University of Pretoria. Redundancy testing is a research evaluation approach in which the survey target population provides the same answers to questions asked, thus resulting in repetitive answers [104]. This was done to ensure reliability and validity but also repeatability of the method adopted. The researcher further instrumentalised the quantitative method through the use of statistical methods, including Factor Analysis (FA) to identify and explore the distribution of data collated from the survey. Chapter 7 details the application of FA in the research.

In order to ensure validity and reliability of the research instrument, different research methods and techniques were adopted. The researcher adopted an expert sampling method. Expert sampling methodology is a research method that draws a population sample from among expert groups or populations. This sampling strategy was chosen based on the researcher's need for expert opinion of certain key populations (judges, expert witnesses, defence lawyers, prosecutors and investigators) whose perspectives on the research subject matter is key to establishing the foundations of the research. Expert sampling was considered to be an optimal way to construct the views of respondents who are considered experts in the subject matter under investigation [106]. The survey was also consensus-oriented, thereby justifying the application of expert sampling for the research [104]. The sample selected is theoretically justified based on a consensus theory approach [107], [108], which is a social science research approach that is based on common understanding and experiences of a population sample.

Experts were drawn from the population sample from different jurisdictions where digital evidence is applied in criminal proceedings. This method was significantly important for the research because similarities in experts' views on the broad subject matter under investigation were counterbalanced by their varied opinions in their areas of expertise [104]. For example, experts who participated in the research were asked to confirm whether the determinants impact the admissibility of digital evidence, after which they were asked to provide their varied opinions on the scale of significance of the determinants in practice. To ensure that respondents understood the meaning of the determinants before completing the survey, the researcher provided explanations of the various determinants in the survey.

The research instrument was also subjected to a number of validity and reliability tests including questionnaire validity, face validity, content validity and construct validity which are essential scientific methods to achieve validity and reliability [109].

Questionnaire validity refers to the accuracy and consistency of questionnaire to provide a reliable research data. Face validity refers to the degree to which a measure appears to be related to a specific construct in research [109]. According to Burton and Mazerolle [110], face validity establishes a research instrument's ease of use, clarity and readability. Contents validity refers to the extent that the survey is relevant and representative of the target construct in a given research. It establishes credibility, accuracy and relevance of the subject matter under investigations [110]. Construct validity establishes a cause and effect relationship in a given research instrument [109].

In operationalising the above research validity methods and techniques, survey questions were reviewed by the research supervisor and relevant amendments were made to truly respond to the objectives of the survey. The review by the supervisor led to a better background information to guide survey respondents with their responses. Pilot tests were conducted involving external experts and respondents. This activity led to the appropriate modification of the questionnaire especially regarding the construction of the survey questions.

Whilst the online survey platform (SurveyGizmo[6]) used made it impossible for the introduction of certain errors especially regarding numerical responses, checks were further conducted on the overall datasets to ensure appropriate values were entered by respondents. In addition to the above, the application of Factor Analysis (FA) itself on the dataset represents another validation of the survey findings. According to Burton and Mazerolle [110], FA is an important analytic research tool to assess construct validity. FA is a useful tool to establish the relationships among variables in a dataset. Its application established the correlations between the various determinants. Detailed findings from the application of the FA on the dataset is presented in Section 7.3.

[6] SurveyGizmo is the online platform used to administer the survey. https://www.surveygizmo.com/

Before conducting FA on the dataset, initial validity tests were performed to establish the suitability of the dataset. This test is known as the Kaiser-Meyer-Olkin (KMO) Sampling Adequacy. Kaiser-Meyer-Olkin (KMO) is a statistical test method used to measure how suitable a data is for FA. The KMO sampling adequacy vary from zero (0) to one (1). According to the KMO sampling adequacy, a value closer to one (1) is better for FA whereas a value close to zero (0) is inappropriate for FA. A KMO sampling adequacy value of 0.77 was obtained, suggesting that the dataset is adequate for the application of FA [111].

The above research methods and techniques ensured the validity and reliability of the research instrument for the construction of the HM-DEAA.

Out of the sample population targeted, a total of 77 respondents participated in the survey. Those who did not respond to the survey did not provide any reasons for their lack of participation. Respondents were drawn from both common law and civil law jurisdictions across Africa, North and South America, Asia, Europe and the Middle East, as shown in Appendix E. Respondents from the following countries participated in the survey: Argentina; Australia; Canada; Costa Rica; Germany; Ghana; Greece; Hong Kong; India; Italy; Kenya; Macau; Malaysia; Netherlands; Pakistan; Paraguay; Philippines; Portugal; Russia; Serbia; Singapore; South Africa; Trinidad and Tobago; United Arab Emirates; United Kingdom; and the United States. Appendix E highlights the distribution of respondents' geographical locations. The significant representation of judges in the survey was motivated by the fact that, the primary focus of the HM-DEAA tool is for judicial decision making in criminal proceedings even though investigators, prosecutors, defence lawyers and even digital forensics expert witnesses should find the HM-DEAA tool useful for evaluating digital evidences with regard to its potential use in court.

Respondents were further asked to indicate the impact of each of the determinants on evidential weight of digital evidence using a Likert scale [105]. Table 6.2 highlights the Likert method adopted and its descriptive relevance to the research.

Table 6.2: Evidential Weight Impact Description using Likert Method

Score	Likert Representation	Description
1	No Impact	The determinant has *no effect* on the digital evidence in question.
2	Minimal Impact	The determinant has *very little effect* on the digital evidence in question.
3	Moderate Impact	The determinant *has some effect but not significant enough* on the digital evidence in question.
4	Significant Impact	The determinant has *considerable effect* on the digital evidence in question.
5	Very Significant Impact	The determinant has *exceptionally impactful effect* on the digital evidence in question.

As mentioned before, respondents were carefully selected from different jurisdictions. Background, knowledge and criminal justice experience involving digital evidence were among the factors considered in sampling respondents based on the expert sampling method adopted [104], [112], [108]. Figures 6.1 and 6.2 contain representations of the background of the experts who participated in the survey.

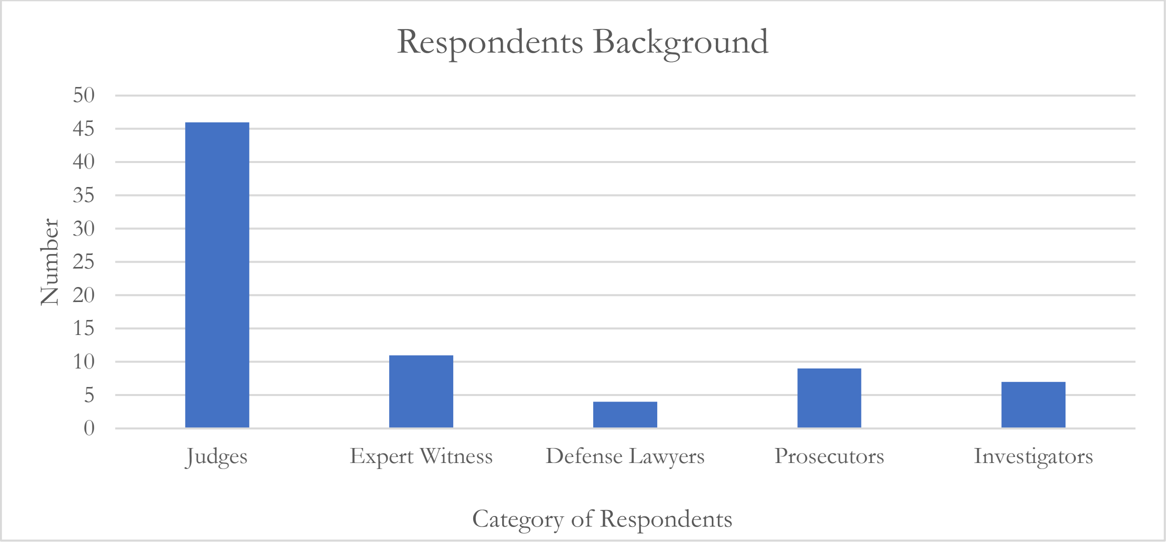


Figure 6.1: Background of Survey Respondents Represented in Numbers

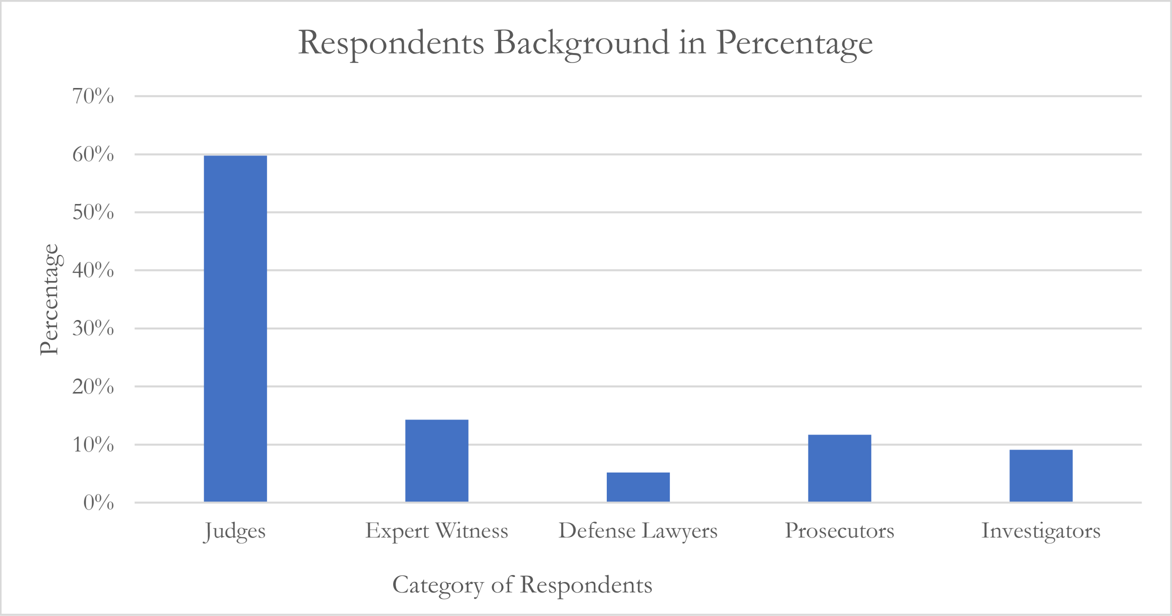


Figure 6.2: Percentage Representation of Respondents Background

From the above distribution, about 60% of respondents who participated in the survey were judges with judicial knowledge and experience in digital evidence. The other survey respondents were drawn from expert witnesses, defence lawyers, prosecutors and investigators (law enforcement). The next section discusses findings from the survey and their impact on the research.

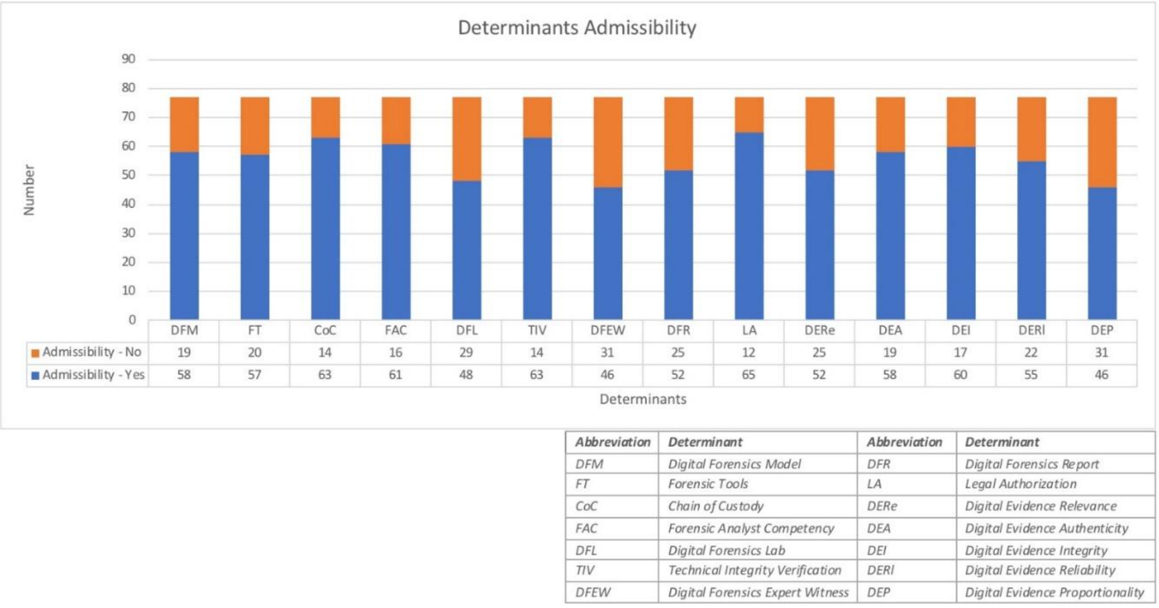
6.4. Survey Findings and Discussions

This section discusses results obtained from the survey. In order to validate research objectives 1 and 4 which state;

(1) What technical determinants underpin the admissibility of digital evidence?

(4) What are the determinants of evidential weight of a piece of digital evidence?

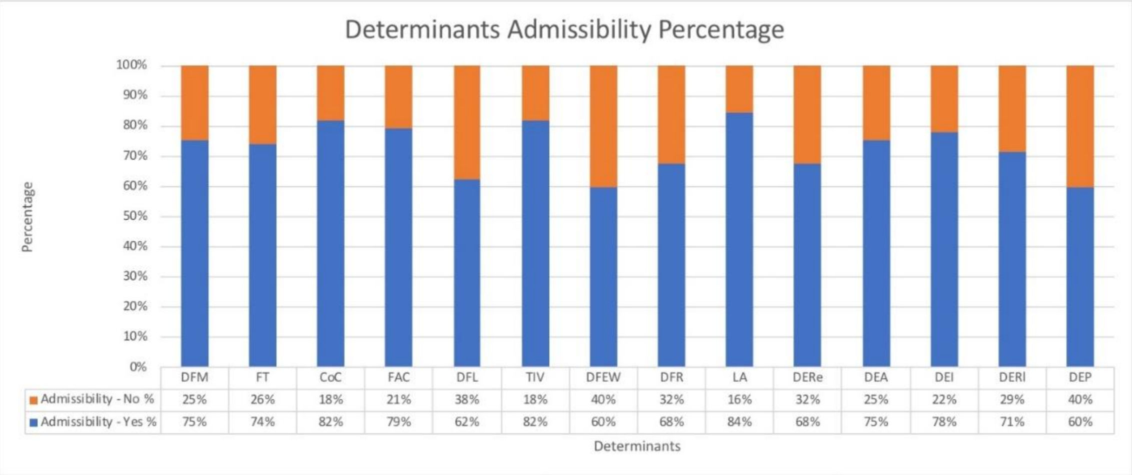
the researcher asked respondents to indicate whether each of the technical and legal determinants presented affect evidence admissibility in a court of law. Figures 6.3 and 6.4 highlight the responses of the experts surveyed.

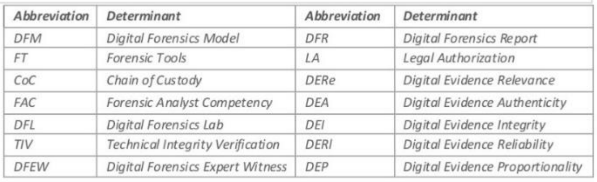


	DFM	FT	CoC	FAC	DFL	TIV	DFEW	DFR	LA	DERe	DEA	DEI	DERI	DEP
■ Admissibility - No	19	20	14	16	29	14	31	25	12	25	19	17	22	31
■ Admissibility - Yes	58	57	63	61	48	63	46	52	65	52	58	60	55	46

Abbreviation	*Determinant*	*Abbreviation*	*Determinant*
DFM	*Digital Forensics Model*	*DFR*	*Digital Forensics Report*
FT	*Forensic Tools*	*LA*	*Legal Authorization*
CoC	*Chain of Custody*	*DERe*	*Digital Evidence Relevance*
FAC	*Forensic Analyst Competency*	*DEA*	*Digital Evidence Authenticity*
DFL	*Digital Forensics Lab*	*DEI*	*Digital Evidence Integrity*
TIV	*Technical Integrity Verification*	*DERI*	*Digital Evidence Reliability*
DFEW	*Digital Forensics Expert Witness*	*DEP*	*Digital Evidence Proportionality*

Figure 6.3: Determinant Admissibility by Number





Abbreviation	Determinant	Abbreviation	Determinant
DFM	Digital Forensics Model	DFR	Digital Forensics Report
FT	Forensic Tools	LA	Legal Authorization
CoC	Chain of Custody	DERe	Digital Evidence Relevance
FAC	Forensic Analyst Competency	DEA	Digital Evidence Authenticity
DFL	Digital Forensics Lab	DEI	Digital Evidence Integrity
TIV	Technical Integrity Verification	DERI	Digital Evidence Reliability
DFEW	Digital Forensics Expert Witness	DEP	Digital Evidence Proportionality

Figure 6.4: Determinant Admissibility by Percentage

The distribution in Figure 6.3 is explained using two determinants. The reader can easily follow the same example to explain the other determinants. From the above distribution, 14 survey participants representing about 18% indicated that CoC does not affect the admissibility of digital evidence in a court of law, while 62 survey participants, representing about 82% indicated that CoC affects evidence admissibility. Regarding the legal determinants, 31 respondents, representing about 40% indicated that DEP does not affect digital evidence admissibility, while 46 participants, representing about 60% indicated the effect of DEP on digital evidence admissibility in a court of law.

A number of factors could have contributed to the above responses. For example, CoC, is a determinant widely recognised by experts as one of the important requirements for digital evidence admissibility. This assertion is confirmed by the high positive response rate of 82% as highlighted in Figure 6.4. However, a total of 18% of respondents indicated that CoC does not affect evidence admissibility. Respondents' understanding as well as the prevailing legal practices in specific jurisdictions may have contributed to the 18% responses who indicated CoC does not affect evidence admissibility. Similarly, prevailing judicial practices in certain jurisdictions as well as exception rules in judicial proceedings could account for the high number of respondents who indicated that DEP does not affect evidence admissibility. For example, not all jurisdictions have introduced human rights safeguards in their criminal legislations and this could affect the consideration of DEP as a legal determinant in such jurisdictions.

From the data presented in Figure 6.4 and the subsequent analysis, the research has established that, knowledge of digital forensics and digital evidence as well as judicial practices and experiences of judicial practitioners impacts on their understandings of the determinants and, subsequently, their considerations relative to the admissibility of digital evidence in a court of law.

To achieve objectives 2 and 5 which state;

(2) What legal determinants underpin the admissibility of digital evidence?

(5) How is the evidential weight of digital evidence determined?

the researcher asked respondents to identify other determinants which were not listed in the survey. Participants listed the following as responses:

1. Authenticity of Digital Evidence
2. Daubert Standard
3. Forensic Tools Licenses
4. Collection of Digital Evidence

5. Integrity of Evidence Source
6. Storage before Production in Court
7. Validation of Forensics Lab
8. Network Traffic Analysis
9. Validation of Tools
10. Location of Digital Evidence

While the above factors are essential and have impacts on digital evidence admissibility, they are essentially factors or requirements that are addressed by the various categories of technical and legal determinants, which are presented in Chapter 4. From the explanations provided by respondents, the above factors are components of the following corresponding determinants, as shown in Table 6.3:

Table 6.3: Suggestions by Survey Respondents and Corresponding Determinants

S/N	Additional Factors/Determinants Identified by Respondents	Determinant Category
1	Authenticity Digital Evidence	Digital Evidence Authenticity Determinant
2	Daubert Standard	Digital Forensics Model Determinant Forensic Tools Determinant
3	Forensic Tools Licenses	Forensic Tool Determinant
4	Collection of Digital Evidence	Chain of Custody Determinant
5	Integrity of Evidence Source	Digital Evidence Integrity Determinant
6	Storage before Production in Court	Chain of Custody Determinant
7	Validation of Forensics Lab	Digital Forensics Lab Determinant
8	Network Traffic Analysis	Digital Forensics Model Determinant
9	Validation of Tools	Forensic Tools Determinant
10	Location of Digital Evidence	Chain of Custody Determinant

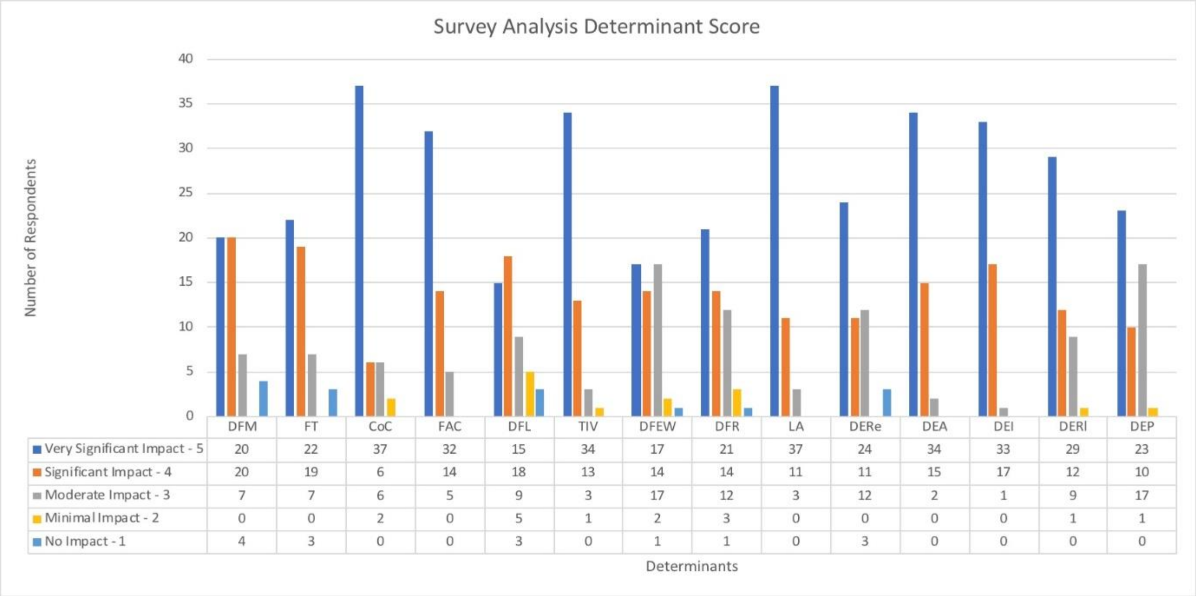
From the analysis, the understanding of the subject area by respondents might have contributed to providing these additional factors, which are essentially part of the existing (given) determinants. For example, validation of tools (additional determinant 9 in Table 6.3) is one of the assessment criteria and expectations for assessing the forensic tools determinant, as shown in Appendix F.

In order to achieve objectives 3 and 6 of the survey which state;

(3) Determine the impact of each of the technical determinants on evidential weight of a piece of digital evidence;

(6) Determine the impact of each of the legal determinants on evidential weight of a piece of digital evidence.

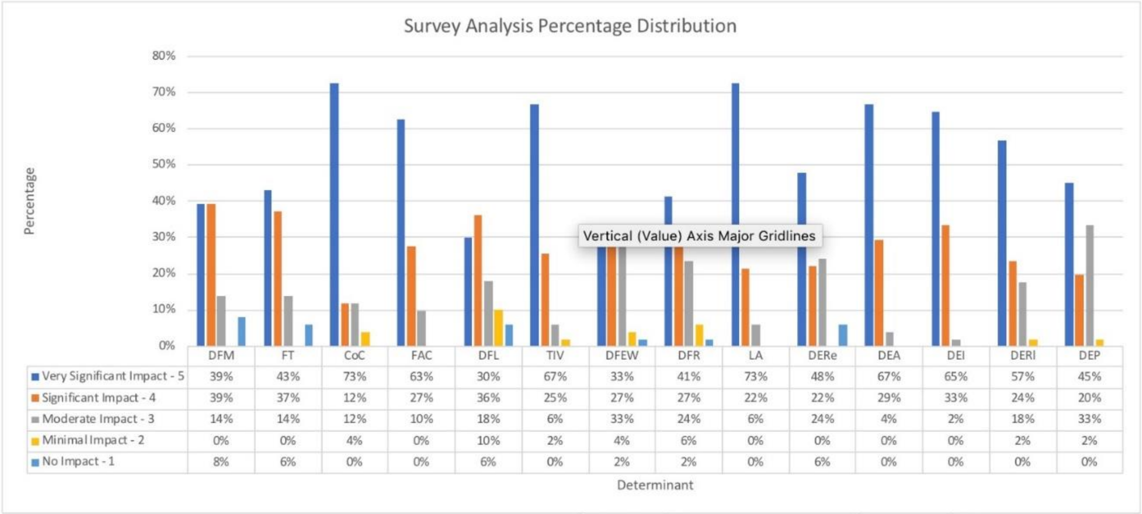
the researcher asked respondents to rate the impact of each of the determinants on the evidential weight of a piece of digital evidence using the Likert scale of 1–5, as explained in Figure 6.2. Figures 6.5 and 6.6 highlight the findings from the survey:



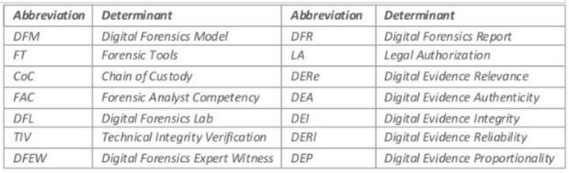
	DFM	FT	CoC	FAC	DFL	TIV	DFEW	DFR	LA	DERe	DEA	DEI	DERI	DEP
Very Significant Impact - 5	20	22	37	32	15	34	17	21	37	24	34	33	29	23
Significant Impact - 4	20	19	6	14	18	13	14	14	11	11	15	17	12	10
Moderate Impact - 3	7	7	6	5	9	3	17	12	3	12	2	1	9	17
Minimal Impact - 2	0	0	2	0	5	1	2	3	0	0	0	0	1	1
No Impact - 1	4	3	0	0	3	0	1	1	0	3	0	0	0	0

Abbreviation	*Determinant*	*Abbreviation*	*Determinant*
DFM	*Digital Forensics Model*	*DFR*	*Digital Forensics Report*
FT	*Forensic Tools*	*LA*	*Legal Authorization*
CoC	*Chain of Custody*	*DERe*	*Digital Evidence Relevance*
FAC	*Forensic Analyst Competency*	*DEA*	*Digital Evidence Authenticity*
DFL	*Digital Forensics Lab*	*DEI*	*Digital Evidence Integrity*
TIV	*Technical Integrity Verification*	*DERI*	*Digital Evidence Reliability*
DFEW	*Digital Forensics Expert Witness*	*DEP*	*Digital Evidence Proportionality*

Figure 6.5: Total Number of Scores Respondents Awarded to each Determinant



	DFM	FT	CoC	FAC	DFL	TIV	DFEW	DFR	LA	DERe	DEA	DEI	DERI	DEP
■ Very Significant Impact - 5	39%	43%	73%	63%	30%	67%	33%	41%	73%	48%	67%	65%	57%	45%
■ Significant Impact - 4	39%	37%	12%	27%	36%	25%	27%	27%	22%	22%	29%	33%	24%	20%
■ Moderate Impact - 3	14%	14%	12%	10%	18%	6%	33%	24%	6%	24%	4%	2%	18%	33%
■ Minimal Impact - 2	0%	0%	4%	0%	10%	2%	4%	6%	0%	0%	0%	0%	2%	2%
■ No Impact - 1	8%	6%	0%	0%	6%	0%	2%	2%	0%	6%	0%	0%	0%	0%



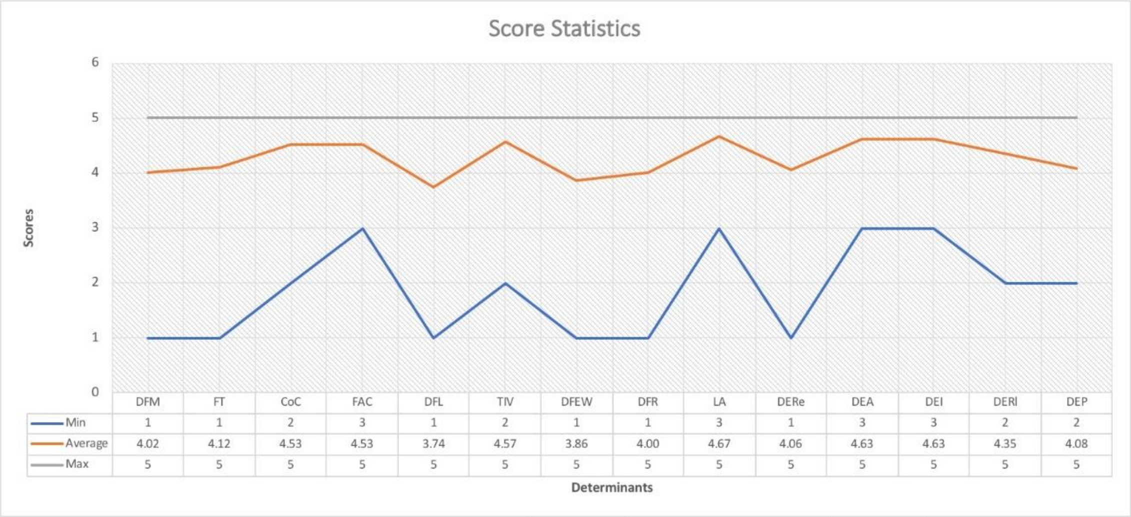
Abbreviation	*Determinant*	*Abbreviation*	*Determinant*
DFM	*Digital Forensics Model*	*DFR*	*Digital Forensics Report*
FT	*Forensic Tools*	*LA*	*Legal Authorization*
CoC	*Chain of Custody*	*DERe*	*Digital Evidence Relevance*
FAC	*Forensic Analyst Competency*	*DEA*	*Digital Evidence Authenticity*
DFL	*Digital Forensics Lab*	*DEI*	*Digital Evidence Integrity*
TIV	*Technical Integrity Verification*	*DERI*	*Digital Evidence Reliability*
DFEW	*Digital Forensics Expert Witness*	*DEP*	*Digital Evidence Proportionality*

Figure 6.6: Percentage Score and Distribution for each Determinant

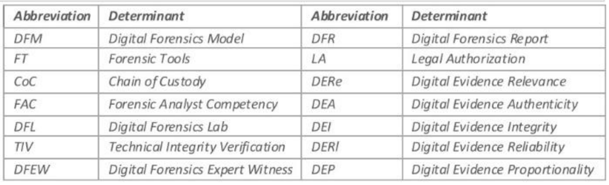
Figure 6.5 highlights the scores attributed to each of the determinants while Figure 6.6 provides the distribution of percentage score associated with each of the determinants respectively. Both figures explain findings from the survey. For example, relative to the CoC determinant, 59 respondents representing about 77% rated its impact on digital evidence with a score of 5 (very significant impact); 6 respondents representing 8% of the survey sample population rated its impact with a score of 4 (significant impact); 9 respondents representing 12% of respondents rated its impact with a score of 3 (moderate impact); 2 respondents representing 3% of respondents rated its impact with a score of 2 (minimal impact) and 1 respondent, representing about 1% of the survey population rated its impact on digital evidence with a score of 1 (no impact).

Similarly for DEP, 34 respondents representing about 44% rated its impact on digital evidence with a score of 5 (very significant impact); 16 respondents representing 21% of the survey sample population rated its impact with a score of 4 (significant impact); 19 respondents representing 25% of respondents rated its impact with a score of 3 (moderate impact); 3 respondents representing 4% of respondents rated its impact with a score of 2 (minimal impact) and the 5 respondents, representing about 6% of the survey population rated its impact on digital evidence with a score of 1 (no impact).

The median score for the various determinants was computed and is highlighted in Figure 6.7.



	DFM	FT	CoC	FAC	DFL	TIV	DFEW	DFR	LA	DERe	DEA	DEI	DERl	DEP
Min	1	1	2	3	1	2	1	1	3	1	3	3	2	2
Average	4.02	4.12	4.53	4.53	3.74	4.57	3.86	4.00	4.67	4.06	4.63	4.63	4.35	4.08
Max	5	5	5	5	5	5	5	5	5	5	5	5	5	5



Abbreviation	*Determinant*	*Abbreviation*	*Determinant*
DFM	*Digital Forensics Model*	*DFR*	*Digital Forensics Report*
FT	*Forensic Tools*	*LA*	*Legal Authorization*
CoC	*Chain of Custody*	*DERe*	*Digital Evidence Relevance*
FAC	*Forensic Analyst Competency*	*DEA*	*Digital Evidence Authenticity*
DFL	*Digital Forensics Lab*	*DEI*	*Digital Evidence Integrity*
TIV	*Technical Integrity Verification*	*DERl*	*Digital Evidence Reliability*
DFEW	*Digital Forensics Expert Witness*	*DEP*	*Digital Evidence Proportionality*

Figure 6.7: Distribution of Scores for each of the Determinants

In Figure 6.7, the minimum, average and maximum scores for each of the determinants are stated. For example, from the responses received, the impact of the CoC determinant on digital evidence admissibility is rated 4.59 on a scale of 1 to 5.

It is important to highlight that from the analysis of data collated, there were no conspicuous variations in the responses provided by the judges and other criminal justice actors relative to the importance of the determinants. This finding explains that all the criminal justice actors considered in the research have a common understanding and expectation of the application of digital evidence in criminal proceedings. However, the level of technical and judicial knowledge and experience is a key factor that impacted the responses provided by survey participants as reflected in the variation of responses provided, especially the effect and the scoring of the determinants considered.

6.5. Conclusion

In this chapter, the researcher presented the foundations of the survey conducted and the findings from collated data. This chapter introduced the methodology adopted for the research and the justification for adopting an integrated scientific methodology. Findings from the survey have validated both the technical and legal determinants introduced in Chapter 4. This is evidenced by the confirmation of the various determinants by the findings from the survey as shown in Figure 6.3 and Figure 6.4. Survey findings have also provided the quantitative data required for further analysis through FA, which are detailed in the next chapter.

Judicial knowledge and experience with digital evidence as well as judicial practices in different jurisdictions have been found to be important factors that influence the application of the determinants relative to digital evidence admissibility assessment in judicial proceedings. The next focus of the thesis is the implementation of the HM-DEAA.

PART 4: HM-DEAA IMPLEMENTATION

The previous three chapters have provided the research foundation for the proposed Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) framework. The next three chapters focus on the implementation of the model. Part Four covers Chapter 7 to Chapter 9. Chapter 7 provides the mathematical foundation of the research through the introduction of an algorithm and Factor Analysis method to operationalise the HM-DEAA model. Chapter 8 introduces an expert system, which the researcher has introduced, to automate the function of the model proposed. Chapter 9 discusses the application of the model to real judicial cases.

CHAPTER 7: IMPLEMENTATION OF THE HM-DEAA

7.1. Introduction

In order to resolve the *techno-legal dilemma* of digital evidence admissibility, which is the focus of the thesis, the abstract Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) model presented and discussed in the preceding chapters to be operationalised. The goal of the HM-DEAA is to provide the criminal justice sector — especially the judiciary — with a judicial tool to facilitate digital evidence admissibility assessment and evidential weight determination. This chapter introduces an algorithm for the operationalization of the HM-DEAA. This chapter also introduces Factor Analysis as a mathematical tool capable of aiding the HM-DEAA model in the determination of evidential weight of digital evidence.

The algorithm being introduced is expected to be used primarily by judges as a judicial tool in criminal proceedings. The algorithm is also expected to serve as a tool for investigators, prosecutors and defence lawyers to evaluate digital evidences with regard to its potential use in court. This chapter explores the operationalisation of the HM-DEAA with the aim of contributing to the digital evidence assessment process in practice, which is the objective underlying the thesis.

The remainder of this chapter is constructed as follows. Section 7.2 presents the algorithm underlying the HM-DEAA model. Section 7.3 discusses the application of Factor Analysis in the research and its contributions to resolving the *techno-legal dilemma*. Section 7.4 evaluates the HM-DEAA algorithm while section 7.5 concludes this chapter with a summary.

7.2. Flow Chart Representation of HM-DEAA Algorithm

In this section, the researcher presents the flow chart, which explains the algorithm underlying the HM-DEAA. The flow chart highlights the logical sequences of the relationship between the various determinants in each of the phases of the HM-DEAA model as presented in Chapter 5. In a practical scenario, the flow chart logically represents the flow of the specific interactions of the various determinants during a typical judicial proceeding. Thus, the flow chart explains the sequential judicial activities relative to the introduction of digital evidence into a court through the various stages of witness presentations and cross examinations to the final determination of the case before the court by a judge or a jury.

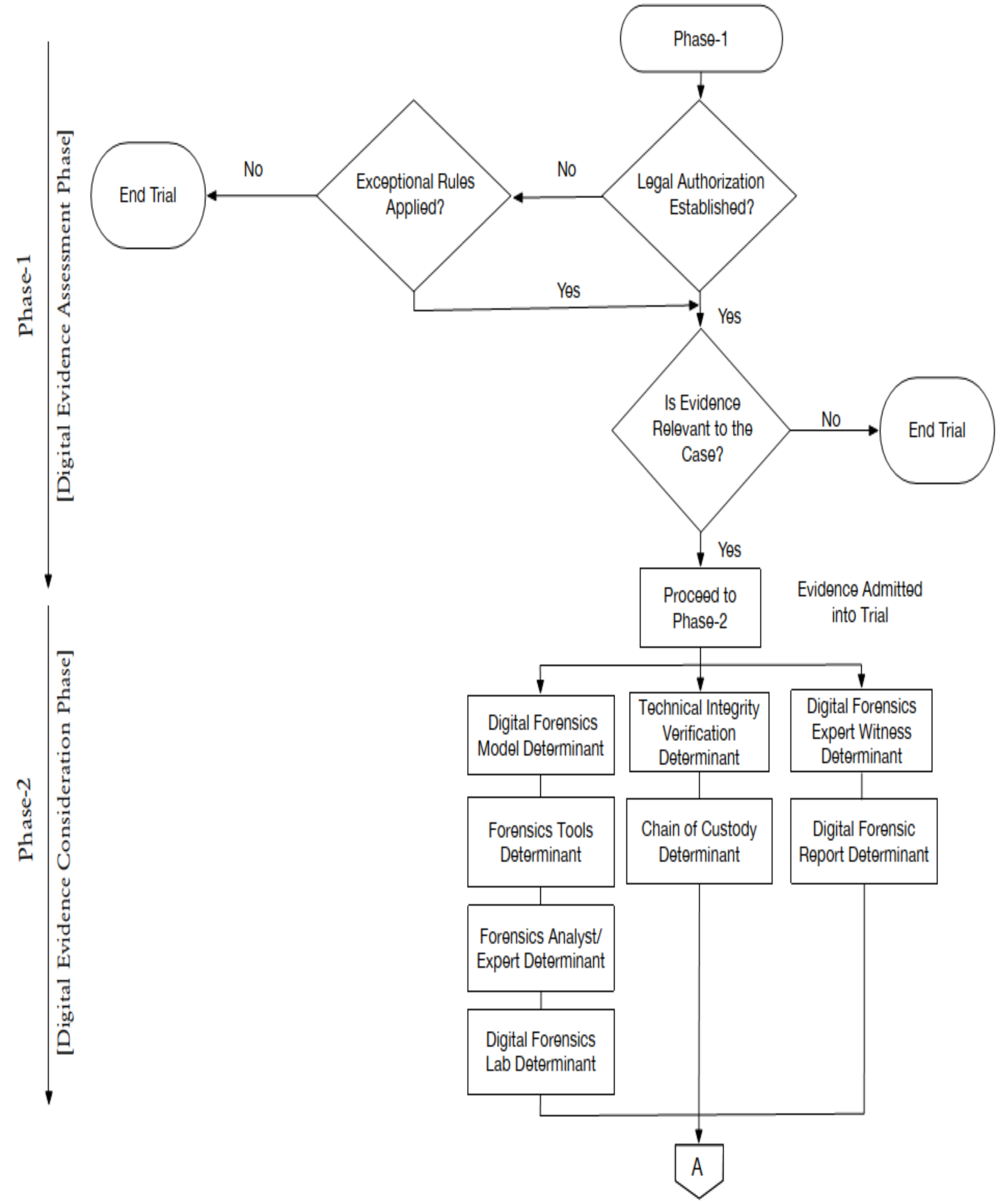

Phase-1
[Digital Evidence Assessment Phase]
Phase-2
[Digital Evidence Consideration Phase]
Phase-1
Legal Authorization Established?
No
Exceptional Rules Applied?
No
End Trial
Yes
Yes
Is Evidence Relevant to the Case?
No
End Trial
Yes
Proceed to Phase-2
Evidence Admitted into Trial
Digital Forensics Model Determinant
Technical Integrity Verification Determinant
Digital Forensics Expert Witness Determinant
Forensics Tools Determinant
Chain of Custody Determinant
Digital Forensic Report Determinant
Forensics Analyst/ Expert Determinant
Digital Forensics Lab Determinant
A

Figure 7.1: Flow Chart representing Digital Evidence Assessment and Digital Evidence Consideration Phases

In the *Digital Evidence Assessment* phase (Phase 1), the legal foundations of digital evidence are established. The relevance of the evidence to the case before the court is determined after legal authorisation is established. This stage constitutes the pre-trial stage in most common law jurisdictions. The trial could be ended at this stage if proper legal foundation is not established. In a typical court environment, the case moves into a full trial in the *Digital Evidence Consideration* phase (Phase 2). The prerequisite requirements, the core requirements and evaluation requirements, which are all technical determinants, as shown in Figure 5.3, are assessed in this phase. The next phase is the *Digital Evidence Determination* phase (Phase 3), as shown in Figure 7.2.

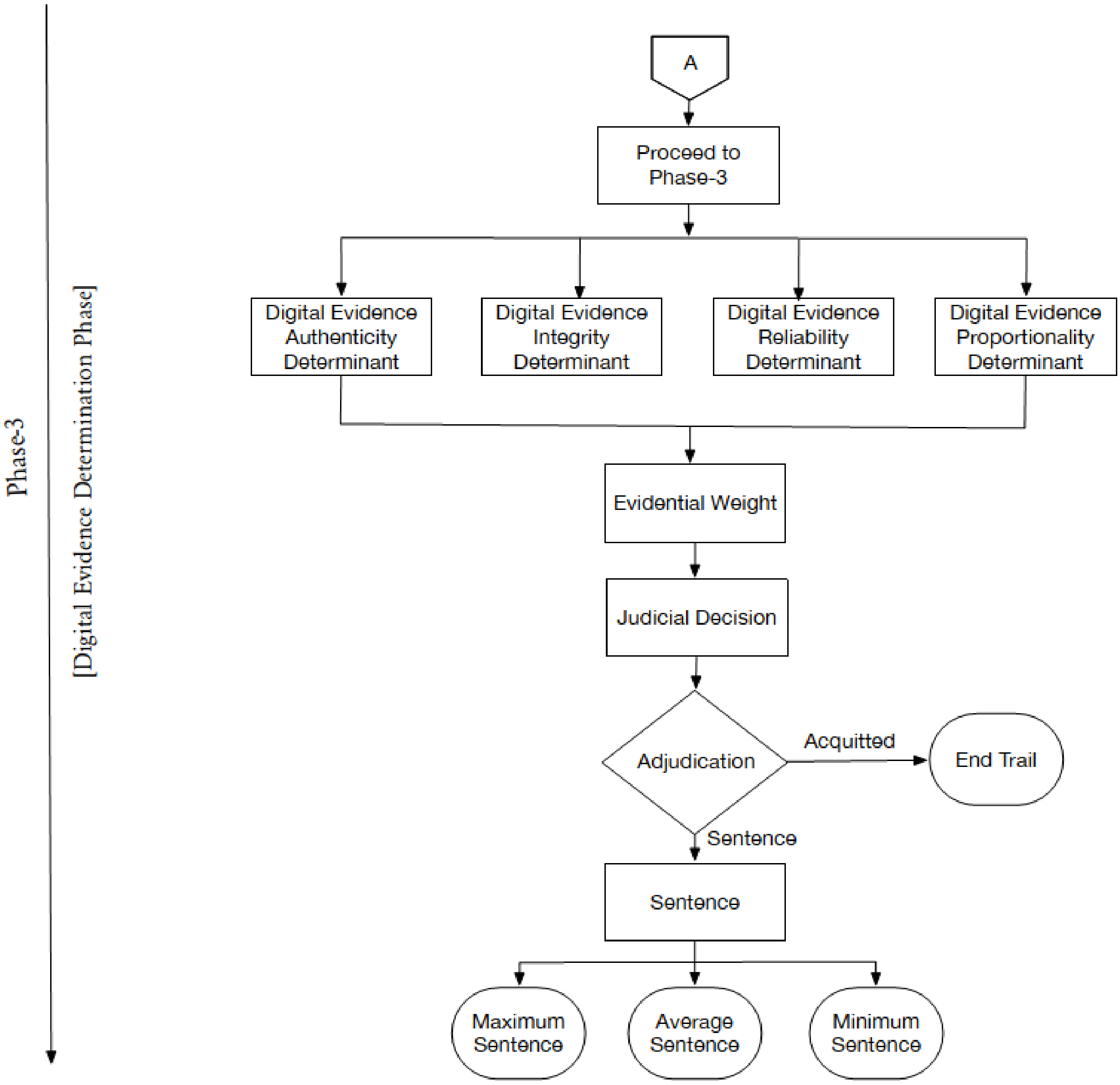

Phase-3
[Digital Evidence Determination Phase]
A
Proceed to Phase-3
Digital Evidence Authenticity Determinant
Digital Evidence Integrity Determinant
Digital Evidence Reliability Determinant
Digital Evidence Proportionality Determinant
Evidential Weight
Judicial Decision
Adjudication
Acquitted
End Trail
Sentence
Sentence
Maximum Sentence
Average Sentence
Minimum Sentence

Figure 7.2: Flow Chart representing Digital Evidence Determination Phase

The determinants in the *Digital Evidence Determination* phase (Phase 3) form the basis of judicial decisions at a trial. In most jurisdictions, the decision could either be *Acquittal* or *Sentencing*. Sentences range from a *maximum, average* or *minimum* based on the evidential weight established through the operationalization of the HM-DEAA as represented in Figure 7.2. In the next section, the researcher presents the foundation of and the formula for determining evidential weight of a piece of digital evidence through the interactions of the various determinants.

7.3. Determination of Evidential Weight using Factor Analysis

Evidential weight is the weight that a judge will normally attach to a particular piece of evidence, which is tendered in a court of law. According to Mason [82], assessing evidential weight involves scrutinizing a piece of evidence and deciding what is acceptable and relevant in arriving at a decision during a trial.

7.3.1. Factor Analysis

The researcher has adopted the Factor Analysis (FA) statistical method to analyze data collated from the survey and to determine the evidential weight of a piece of evidence. FA involves grouping similar variables into dimensions. This process is used to identify latent variables or constructs. The purpose of FA is to reduce many individual items into a fewer number of dimensions. FA can be used to simplify data, such as reducing the number of variables in regression models. The two main FA techniques are Confirmatory Factor Analysis (CFA) and Exploratory Factor Analysis (EFA). CFA attempts to confirm hypotheses and uses path analysis diagrams to represent variables and factors, whereas EFA tries to uncover complex patterns by exploring the dataset and testing predictions [108].

FA is based on groupings of different indices that assess a similar phenomenon [113]. It has been adopted for this research because of its appeal in exploratory data analysis. The main reason for adopting FA as a research method was to summarise the dataset collected from the survey so that relationships and patterns between the determinants can be statistically analyzed, interpreted and understood. FA enabled the regrouping of the determinants into a limited set of clusters based on shared variance. FA has been adopted in this research to construct the weights of the various variables required for making judicial decisions. Findings from the survey presented in Chapter 6 provided the required data to construct the theoretical framework to operationalise the FA [112].

In order to perform FA, there must be univariate and multivariate normality within the data [108]. In statistical analysis, univariate normality refers to a single variable present in the dataset while the multivariate normality refers to multiple variables present in the dataset. In this context, the dataset refers to data collated from the survey. It is also important that there is an absence of univariate and multivariate outliers (i.e., a data point in a set of results that is very much bigger or smaller than the next nearest data point) [114]. A univariate outlier is a data point that consists of an extreme value on one variable whilst multivariate outlier is a combination of unusual scores on at least two variables. This could occurred due to wrong data entry [115]. Also, determining factors are based on the assumption that, there is a linear relationship between the factors and the variables when computing the correlations [116]. Before applying FA to the dataset, there should be some correlation between the determinants. Hence, the correlation between the determinants were computed using the Pearson Correlation Coefficient [117].

The Pearson Correlation Coefficient is a very useful statistical formula that measures the strength between variables and relationships. This Pearson Correlation Coefficient formula in equation 7.1 was used to determine the correlation between the determinants. This method enabled the determination of the number of factors between the data. The general formula for computing the correlation using Pearson Correlation Coefficient is given as follows.

Equation 7.1: Pearson Correlation Coefficient Formula

$$r = \frac{N\sum xy - (\sum x)(\sum y)}{\sqrt{[N\sum x^2 - (\sum x)^2][N\sum y^2 - (\sum y)^2]}} \tag{7.1}$$

Where:

r = correlation coefficient

N = number of pairs of scores

$\sum$xy = sum of the products of paired scores

$\sum$x = sum of x scores

$\sum$y = sum of y scores

$\sum x^2$ = sum of squared x scores

$\sum y^2$ = sum of squared y scores

Assuming computation of correlation between the Digital Forensics Model (DFM) determinant and the Forensic Tools (FT) determinant, the formula given in equation 7.1 is interpreted as follows:

r = the correlation coefficient between DFM and FT

x = the value of each response by the survey respondents for DFM

y = the value of each response by the survey respondents for FT

xy = the product of the value of both x and y

$\sum x$ = the summation of all values of x

$\sum y$ = the summation of all values of y

$\sum xy$ = the summation of all the products of xy

$\sum x^2$ = the summation of the square of all x

$\sum y^2$ = the summation of the square of all y

N = the total number of respondents to the survey

Equation 7.1 is adopted to determine the correlation between the determinants, which will establish the basis for FA to be applied.

Due to the size of the dataset (i.e., the data from the survey), a statistical software package known as Stata [118] was used to determine the correlation among the data. Stata [118] is an integrated statistical software package that provides various functionalities for data analysis. Correlation measures the extent to which two variables are related. The determinants were initially divided into two variables, namely technical and legal determinants. The Stata software [118] was used to determine the correlations between the variables. This was done primarliy to establish whether the dataset was suitable for FA.

For FA to be applied to a dataset, there should be a correlation between the variables. Analysis of the data generated through the Pearson correlation analysis confirms a correlation between the variables (determinants). Detailed results from the Pearson correlation analysis are presented in Appendix G. From the analysis (as shown in Appendix G), a correlation of 0.324962 has been established between Forensics Tools (FT) and Digital Forensics Model (DFM), which are technical determinants. Also, a correlation of 0.510916 exists between the Digital Evidence Integrity (DEI) and

Digital Evidence Reliability (DERl), which are both legal determinants. In addition, a correlation of 0.500934 exists between the Legal Authorisation (LA) and Technical Integrity Verification (TIV), which are legal and technical determinants respectively. The general guide for interpreting the strength of correlation of coefficient with absolute values as in the dataset is that, a correlation coefficient between 0–0.2 is weak, 0.2–0.4 is mild, 0.4–0.6 is moderate, 0.6–0.8 is strong, 0.8–1.0 is very strong [119]. As a result, it can be stated that, there are mild to moderate correlations among the determinants considered for the analysis.

This correlation further explains a fact that, a survey respondent is likely to provide, for example, a higher score for DEI if the respondent provided a higher score to DERl and vice versa. The procedure of calculating the correlation is provided in Appendix G. The above examples confirm a correlation between the determinants hence FA can be applied to the dataset. As discussed in Section 6.3, a Kaiser-Meyer-Olkin (KMO) Sampling Adequacy test was conducted on the dataset. The test established a sampling adequacy ratio of 0.77. This value confirmed the adequacy of the dataset for FA [111].

7.3.2. Determination of Factors within the Dataset

Once the initial assessment has confirmed the suitability of the dataset for FA, the factors (patterns of responses) in the dataset have to be determined. These factors will later be scored and used to compute the evidential weight. The key concept of FA is that multiple observed variables (determinants) have similar patterns of responses because they are all associated with a latent (i.e., not directly measured) variable. In every FA, there are the same number of factors as there are variables. This is because the number of factors are estimated based on the number of variables (determinants) within the dataset. The factors are not necessarily the dertminants, however, they are patterns of responses that explain the variances for each variable. This implies that some determinants will be relavant and suitable for FA.

In order to determine which factor is relavent for FA, the eigenvalues of the factors have to be detemined. A statistical application was used to determine the eigenvalues of the factors from the dataset, as shown in Table 7.1.

Table 7.1: Eigenvalues

Eigenvalues	
	Eigenvalues
Factor1	4.774696
Factor2	0.626843
Factor3	0.513511
Factor4	0.356166
Factor5	0.278165
Factor6	0.202406
Factor7	0.160997
Factor8	0.101796
Factor9	0.088571
Factor10	-0.01429
Factor11	-0.04106
Factor12	-0.21072
Factor13	-0.23923
Factor14	-0.35143

The eigenvalues is a measure of how much a factor explains the variance of the observed variables (determinants). In addition, Kaiser's selection criterion was adopted for the selection of the relevant factors based on the results from the eigenvalues computation. Kaiser's selection criterion is a statistical selection method for extracting significant factors from a dataset. Kaiser's selection criterion suggests that, any factor with an eigenvalue ≥ 1 explains more variance than a single observed variable, hence any factor with eigenvalues <1 has to be dropped or ignored [120].

From the eigenvalues produced by the analysis, as shown in Table 7.2, the only eigenvalue greater than 1 was Factor1 (4.774696). This factor can therefore be selected to compute the evidential weight using the FA. The next section discusses how the 14 variables (determinants) are scored in order to determine the evidential weight of an evidence.

7.3.3. Factor Score

A factor score can be considered to be a value that describes how much a survey participant would score on a factor. One of the methods to produce a factor score is the Bartlett method (or regression approach) [121]. Table 7.2 shows the factor score, which was generated through the statistical analysis using the Stata application.

Table 7.2: Factor Score Generated by Stata Application

	Factor Score
DFM	0.247633
FT	0.412889
CoC	0.344163
FAC	0.372313
DFL	0.212455
TIV	0.371712
DEFW	0.237606
DFR	0.32664
LA	0.240957
DERe	0.193218
DEA	0.495371
DEI	0.611801
DERl	0.332325
DEP	0.375614

The FA is given by a linear relationship with the latent factors observed in the data from the survey (i.e., investigating whether the number of variables of interest — "the determinants" — are linearly related to a smaller number of observable factors "factor score" dataset).

In general terms,

Equation 7.2: Factor Analysis

$$Factor_{ni} = b_1X_{1i} + b_2X_{2i} + \cdots + b_nX_{ni} + e_i \qquad (7.2)$$

Where $Factor_{ni}$ is denoted by factors present in the data, b denoted by factor loadings (i.e., the factor scores), X is denoted by various determinants, i is denoted by number of observations (i.e., number of factors), and n is denoted by number of variables (i.e., number of determinants).

From the above, a co-efficient formula to run the FA is generated;

Equation 7.3: Factor Analysis of Determinants

$$\begin{aligned} Factor\ Analysis\ of\ Determinants \\ = b_1DFM + b_2FT + b_3CoC + b_4FAE + b_5DFL \\ + b_6TIV + b_7DFEW + b_8DFR + b_9LA + b_{10}DERe \\ + b_{11}DEA + b_{12}DEI + b_{13}DERI + b_{14}DEP + ei \end{aligned} \tag{7.3}$$

where b is denoted by the factor loading. The equation above is the equation the researcher seeks to estimate by FA. The b's from this equation are used to calculate the weights in equation 7.4.

Equation 7.4: Evidential Weight (EW) Determination

$$\begin{aligned} Evidential\ Weight\ (EW) Determination \\ = w_1DFM + w_2FT + w_3CoC + w_4FAE + w_5DFL \\ + w_6TIV + w_7DFEW + w_8DFR + w_9LA + w_{10}DERe \\ + w_{11}DEA + w_{12}DEI + w_{13}DERI + w_{14}DEP + ei \end{aligned} \tag{7.4}$$

where w is denoted by the evidential weight. The next section explains how w (i.e., evidential weight) is calculated.

7.3.4. Calculating Evidential Weight

The evidential weight *(Wd)* is therefore calculated based on equation 7.5, where "b" is the factor score which was generated after running the factor analysis, *i* is the determinant and *total variance* is the sum of the square of the b's (factor scores) as shown in Table 7.3.

Equation 7.5: Evidential Weight

$$\boldsymbol{W_i} = \frac{bn^2}{Total\ Variance} \tag{7.5}$$

Table 7.3: Calculation of Total Variance

	Factor Score	Variance (bn^2)	Determinant Weight (Wd)
DFM	0.247633	0.061322	0.034
FT	0.412889	0.170477	0.095
CoC	0.344163	0.118448	0.066
FAC	0.372313	0.138617	0.025
DFL	0.212455	0.045137	0.077
TIV	0.371712	0.13817	0.077
DEFW	0.237606	0.056457	0.031
DFR	0.32664	0.106694	0.059
LA	0.240957	0.05806	0.032
DERe	0.193218	0.037333	0.021
DEA	0.495371	0.245393	0.136
DEI	0.611801	0.3743	0.208
DERl	0.332325	0.11044	0.061
DEP	0.375614	0.141086	0.078
Total Variance		**1.801933612**	

For example, to calculate the evidential weight for Digital Forensic Model (DFM), the evidential weight is calculated as follows;

$$\boldsymbol{W_i} = \frac{bn^2}{Total\ Variance}$$

$$\boldsymbol{W_{DFM}} = \frac{(0.247633)^2}{1.801933612}$$

$$\boldsymbol{W_{DFM}} = 0.034031203$$

Table 7.3 shows the calculation of total variance and the results of the calculations of evidential weight (Wd) for the determinants.

The next section evaluates the HM-DEAA algorithm using a hypothetical case.

7.4. HM-DEAA Algorithm Evaluation

The researcher has applied the above equations to a hypothetical case in which digital evidence is involved. The results from the application of FA on the case are shown in Table 7.4.

Table 7.4: Evidential Weight Determination and Analysis

Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Weighted Value (Wv)
DFM	0.034	3.8	0.129
FT	0.095	4.5	0.428
CoC	0.066	3.0	0.198
FAC	0.025	2.5	0.063
DFL	0.077	3.4	0.262
TIV	0.077	2.3	0.177
DFEW	0.031	5.0	0.155
DFR	0.059	4.7	0.277
LA	0.032	3.7	0.118
DERe	0.021	4.2	0.088
DEA	0.136	4.0	0.544
DEI	0.208	2.4	0.499
DERI	0.061	3.6	0.220
DEP	0.078	3.5	0.273
Total Evidential Weight (TEW)			**3.431**

From Table 7.4, the *Determinant Weight (Wd)* denotes the weight for each of the determinants as established through the FA.

The *Determinant Score (Sd)* represents the score assigned to each of the determinants by the court for the case in question. The *Sd* is computed using equation 7.6,

Equation 7.6: Determinant Score (Sd)

$$\text{Determinant Score(Sd)} = \frac{\text{Sum of Assessment Score}}{\text{Total Mark}} * 5 \qquad (7.6)$$

Each determinant has a maximum mark allocation of five (5). Each of the determinants is then assessed by the court using different parameters, which are essentially the key questions addressed during evidence presentation and cross-examination. For example, relative to the Digital Forensics Tool (FT) determinant, the following are among the key questions to determine the score: Which forensics tool(s) was/were used for the forensic examination? Was the tool used licensed? Did you use open source or proprietary software? What is the implication of the use of any of the tools? Was the tool used tested/validated? Do we know the error rate of the tool? What is the level of acceptance of the tool among researchers and digital forensics practitioners? Is there any scientific publication on the tool?

These questions or parameters are determined by the scientific and industry requirements for the acceptance of a forensic tool to conduct digital investigations. While the above questions are not exhaustive, they constitute some of the key assessment parameters for the court to provide a score for the given determinant. Thus, the determinant score value of 4.5 for the FT was generated by applying the equation 7.6. This value constitutes the score assigned by the court after the assessment of the FT determinant based on the assessment questions.

The *Weighted Value (Wv)* represents the evidential weight of each of the determinants. From Table 7.6 the following formula from equation 7.4 applies in calculating the evidential weight:

$$Evidential\ Weight\ (EW)\ Determination$$

$$= w_1DFM + w_2FT + w_3CoC + w_4FAE + w_5DFL + w_6TIV + w_7DFEW + w_8DFR + w_9LA + w_{10}DERe + w_{11}DEA + w_{12}DEI + w_{13}DERI + w_{14}DEP + ei$$

$$= 0.034\ DFM + 0.095\ FT + 0.066\ CoC + 0.025\ FAE + 0.077\ DFL + 0.077\ TIV + 0.031\ DFEW + 0.059\ DFR + 0.032\ LA + 0.021\ DERe + 0.136\ DEA + 0.208\ DEI + 0.061\ DERI + 0.078\ DEP$$

From the above,

Equation 7.7: Weighted Value (Wv)

$$\textbf{Weighted (Wv)} = Determinant\ Weight\ (Wd)\ *\ Determinant\ Score\ (Sd) \tag{7.7}$$

Total Evidential Weight is given by:

Equation 7.8: Total Evidential Weight

$$\sum_{i=1}^{n} Wd_iSd_i = Wd_1Sd_1 + Wd_2Sd_2 + Wd_3Sd_3 + \cdots + Wd_nSd_n \tag{7.8}$$

Where i = Determinants, Wd = Determinant Weight and Sd = Determinant Score.

From Table 7.5,

$$Evidential\ Weight = (0.034 * 3.8) + (0.095 * 4.5) + (0.066 * 3) + \ldots + (0.078 * 3.5)$$

Therefore, EW is **3.431**

Expressing the EW in percentage,

Equation 7.9: EW in Percentage

$$\frac{EW}{5} * 100 \tag{7.9}$$

$$= \frac{3.431}{5} * 100\% = \ 68.63\%$$

The 3.431 representing 68.63% constitutes the *Evidential Weight (EW)* of the piece of evidence tendered in the court. In our hypothetical case presented, the EW provides the basis for a judicial decision. However, it should be noted that, judicial decisions are also impacted by other mitigating factors. The potential impact of these factors on final judicial decisions is discussed in detail in Chapter 8. The percentage value of the EW established above is expected to guide the court on the level of sentencing, which can be *maximum, average* or *minimum* sentence. The EW value is expected to guide the court on sentencing, taking all other mitigating factors into consideration.

7.5. Conclusion

This chapter has introduced the algorithm to operationalise the HM-DEAA including the prospect of customizing the model to determine the evidential weight of a digital evidence in a specific jurisdiction. The algorithm has been applied to a hypothetical case and the analysis of evidential weight determination based on FA has been presented. The relevance of the Evidential Weight (EW) obtained through the hypothetical case has been explained and the implications of the EW in criminal proceedings established.

It is important to highlight that developments in the field of digital forensics could impact on the data generated from the survey to compute the weights for the determinants through the application of the FA. In addition, because the survey conducted to obtain the foundation for the FA analysis was carried out at a certain point in time, and therefore its validity is limited to a certain timeframe. These issues could impact the validity of the HM-DEAA model based on the degree of change recorded both in law and in computing and information technology. The researcher has however proposed future research to address this drawback. This is further discussed in Chapter 10. The next chapter introduces the HM-DEAA expert system, which is designed to operationalise the model.

CHAPTER 8: HM-DEAA EXPERT SYSTEM

8.1. Introduction

The Harmonised Model for Digital Evidence Admissibility Assessment Expert System (HM-DEAA ExP) is a judicial tool for assessing admissibility and evidential weight of digital evidence in criminal proceedings. The application is underpinned by the various technical and legal determinants, which constitute the foundation of digital evidence admissibility. The HM-DEAA ExP is introduced to allow for the practical utilization of the HM-DEAA model in criminal proceedings. The HM-DEAA ExP also allows criminal justice practitioners such as investigators, prosecutors and defence attorneys to evaluate digital evidence, which is introduced to a court during a trial.

This chapter reviews the HM-DEAA ExP, comprising its architecture as a judicial tool and its practical application in judicial proceedings. The remainder of this chapter is constructed as follows: Section 8.2 presents a case scenario for the application of the HM-DEAA ExP. Section 8.3 examines the HM-DEAA ExP model, while Section 8.4 discusses the HM-DEAA ExP algorithm and system requirements. Section 8.5 discusses the operational parameters for the HM-DEAA ExP. Sections 8.6 focuses on HM-DEAA ExP deployment and evaluation while Section 8.7 concludes this chapter with a summary.

8.2. Case Scenario and Purpose of HM-DEAA Expert System

In a typical case scenario, a financial fraud incident involving the fraudulent transfer of funds was investigated by a law enforcement agency. Two suspects were arrested, and their computer devices and mobile phones were lawfully seized by investigators. The devices were forwarded to forensic examiners at the police digital forensics lab for forensic examination. Among other relevant evidences, forensic examiners retrieved fictitious invoices, fraudulent e-mail communications, web browser information, banking and credit card information related to the case as well as a cache of Skype conversations involving the two suspects. Police investigators prepared their forensic reports, which were forwarded to the prosecutions department who proceeded to court with the available evidence.

Upon the examination of the case docket, the prosecution team charged the suspects with defrauding by false pretense and other money laundering related offenses. A pre-trial was conducted and the court established a prima facie[7] case against the suspects. The case went through the normal criminal proceedings, which allowed the prosecutors to make their cases for cross examination by the defence counsel. At a point during the trial, the court invited a technical expert witness to testify on some of the most contentious issues relative to the forensic report submitted by the law enforcement agency. One of the key issues was whether it was possible for someone else to exchange the fraudulent e-mails through the suspects' computers without their knowledge. After several days of the trial, the judge adjourned proceedings, went on recess and returned with his judgement.

The judge had a unique challenge: that of making a judicial decision based on his knowledge of case law but also the evidence before the court. The judge was particularly aware that judicial decisions in such cases are also motivated by the *scientificity* of the technical issues involved, including the attribution of specific user activities to the suspects, which eventually brought in an expert witness to testify.

[7] In most common law jurisdictions, prima facie refers to evidence that, unless rebutted, would be sufficient to prove a particular fact of the case presented before the court or a judge.

HM-DEAA ExP is designed to assist the judge with the case presented above. As a judicial tool, the HM-DEAA ExP, is meant to assist the judge in appraising the various legal and technical arguments presented at the trial for the purposes of establishing the admissibility of the digital evidence presented in the case and also to determine the overall evidential weight in order to arrive at a justifiable judicial decision. The system allows judges to ascertain the *fit for purposeness* of any digital evidence presented during the trial through the assessment of each of the technical and legal determinants, which are the foundational pillars of digital evidence. The HM-DEAA ExP is also designed to allow judges to establish the evidential weight of a piece of evidence. Apart from the judicial use of the tool as explained above, prosecutors, investigators and defence lawyers could use the HM-DEAA ExP to evaluate any digital evidence for its potential use in a court of law. The next section examines the design underlying the HM-DEAA ExP.

8.3. HM-DEEA Expert System Model

A schematic diagram of the HM-DEAA ExP is presented in Figure 8.1.

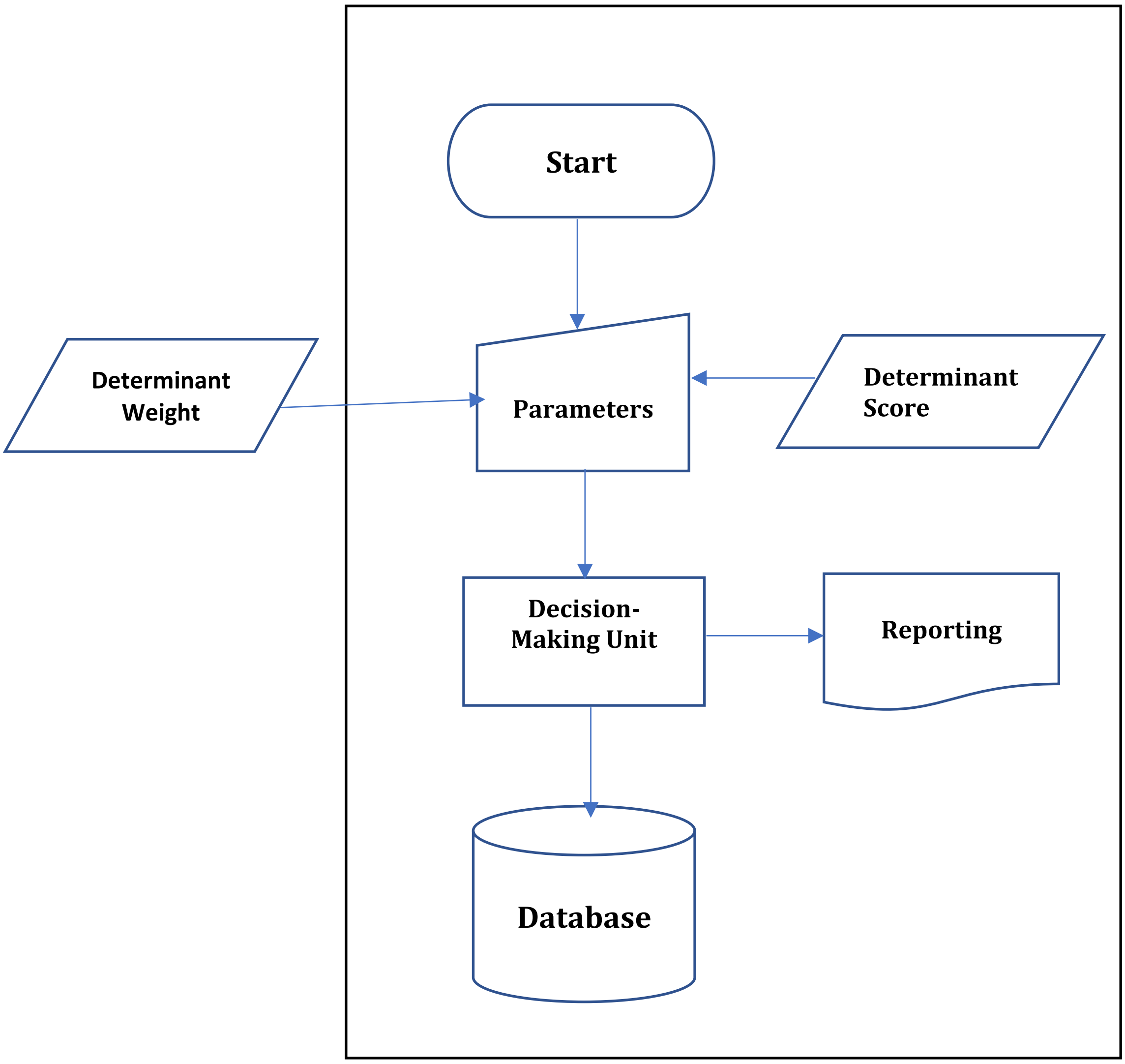
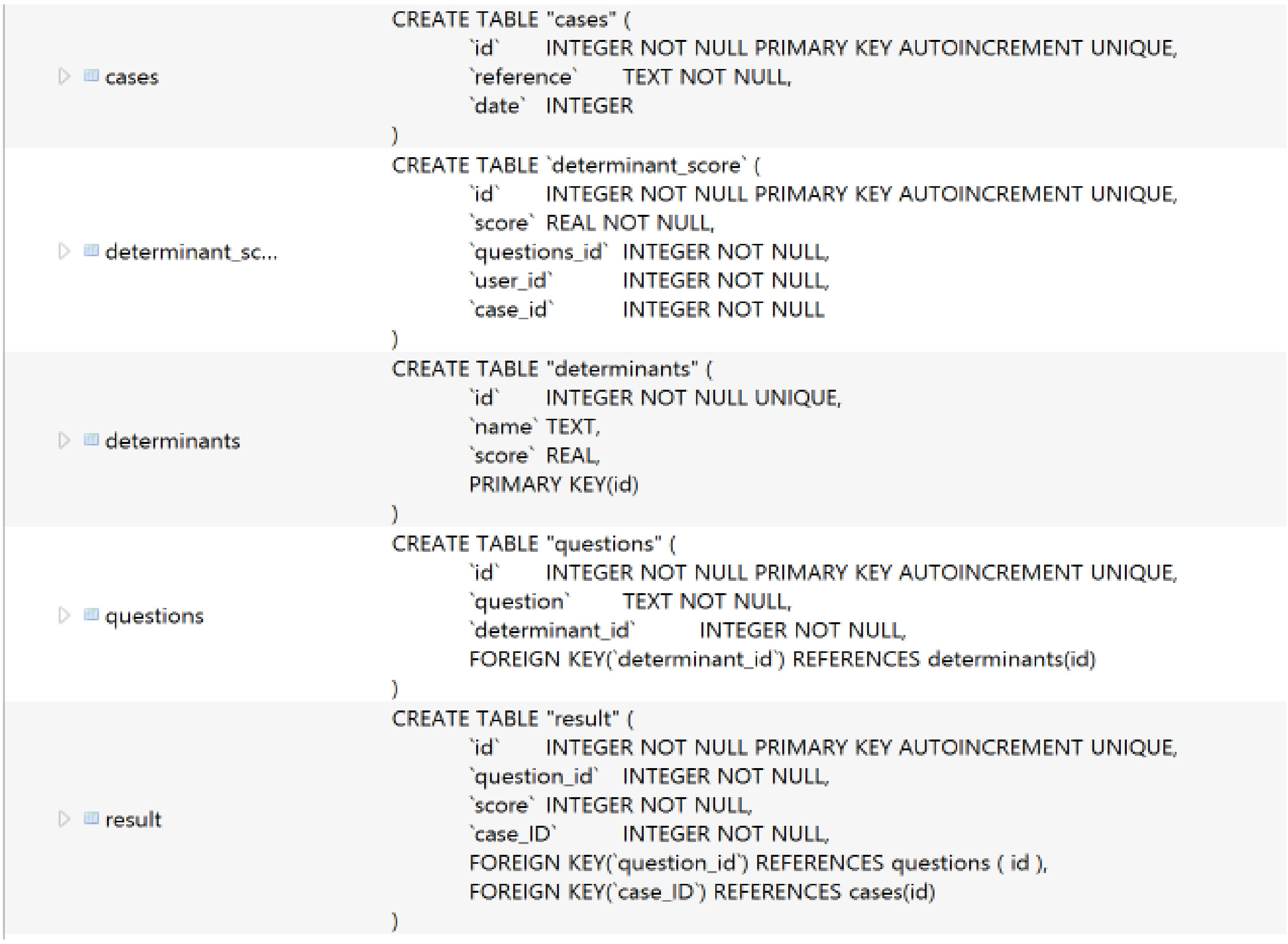


Figure 8.1: Schematic Diagram of the HM-DEAA ExP

The HM-DEAA ExP is graphically depicted in Figure 8.1. The system receives input from statistical software such as the Stata or IBM SPSS (a statistics application). The statistical software is used to compute the *Determinant Weights* for all the determinants by applying Factor Analysis as shown in the previous chapter. The values of each of the determinants are manually inputted into the expert system. The system then receives another input: *Determinant Scores* from the user. The

Determinant Scores are then generated by the expert system for each determinant through assessment of the digital evidence in question.

The *Decision-Making Unit* of the application runs an algorithm on the data pertaining to both the *Determinant Weights* and *Determinant Scores* after which a decision is made. The result of the decision is displayed as a report and saved in the database. Configurations of the system are also saved in the database for reference purposes. All records are stored in an SQLite database. The structure of the HM-DEAA ExP is represented in Figure 8.2.



▷ cases

```
CREATE TABLE "cases" (
          `id`      INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT UNIQUE,
          `reference`      TEXT NOT NULL,
          `date`   INTEGER
)
```

▷ determinant_sc...

```
CREATE TABLE `determinant_score` (
          `id`      INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT UNIQUE,
          `score`  REAL NOT NULL,
          `questions_id`  INTEGER NOT NULL,
          `user_id`         INTEGER NOT NULL,
          `case_id`         INTEGER NOT NULL
)
```

▷ determinants

```
CREATE TABLE "determinants" (
          `id`      INTEGER NOT NULL UNIQUE,
          `name` TEXT,
          `score`  REAL,
          PRIMARY KEY(id)
)
```

▷ questions

```
CREATE TABLE "questions" (
          `id`      INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT UNIQUE,
          `question`      TEXT NOT NULL,
          `determinant_id`         INTEGER NOT NULL,
          FOREIGN KEY(`determinant_id`) REFERENCES determinants(id)
)
```

▷ result

```
CREATE TABLE "result" (
          `id`      INTEGER NOT NULL PRIMARY KEY AUTOINCREMENT UNIQUE,
          `question_id`   INTEGER NOT NULL,
          `score`  INTEGER NOT NULL,
          `case_ID`         INTEGER NOT NULL,
          FOREIGN KEY(`question_id`) REFERENCES questions ( id ),
          FOREIGN KEY(`case_ID`) REFERENCES cases(id)
)
```

Figure 8.2: Snapshot of the Database Structure

The next section examines the algorithm underlying the HM-DEAA ExP and the system requirements.

8.4. HM-DEAA ExP Algorithm and System Requirements

The algorithm underlying the HM-DEAA ExP is explained in Chapter 7. Some of the equations and calculation formulas are repeated here to show the calculations for the case scenario at hand. From the explanations, the *Determinant Weight (Wd)* denotes the weight for each of the determinants, which was established through Factor Analysis. The *Determinant Score (Sd)*, which is represented by:

$$\text{Determinant Score(Sd)} = \frac{\text{Sum of Assessment Score}}{\text{Total Mark}} * 5$$

In addition, *Total Evidential Weight* is given by:

$$\sum_{i=1}^{n} Wd_i Sd_i = Wd_1 Sd_1 + Wd_2 Sd_2 + Wd_3 Sd_3 + \cdots + Wd_n Sd_n$$

Where i = Determinants, Wd = Determinant Weight and Sd = Determinant Score.

Expressing the EW in percentage, $= \frac{EW}{5} * 100$

The Determinant Weights, which were established through factor analysis and presented in Figure 7.5, forms an important component of the HM-DEAA ExP. The HM-DEAA ExP operates with specific system requirements. The tool is a desktop-based application programmed with the Microsoft C# programming language. The application runs on the Microsoft Windows Operating System with the appropriate version of the .Net framework installed. For the HM-DEAA ExP application to run successfully, the requirements listed in Table 8.1 should be met.

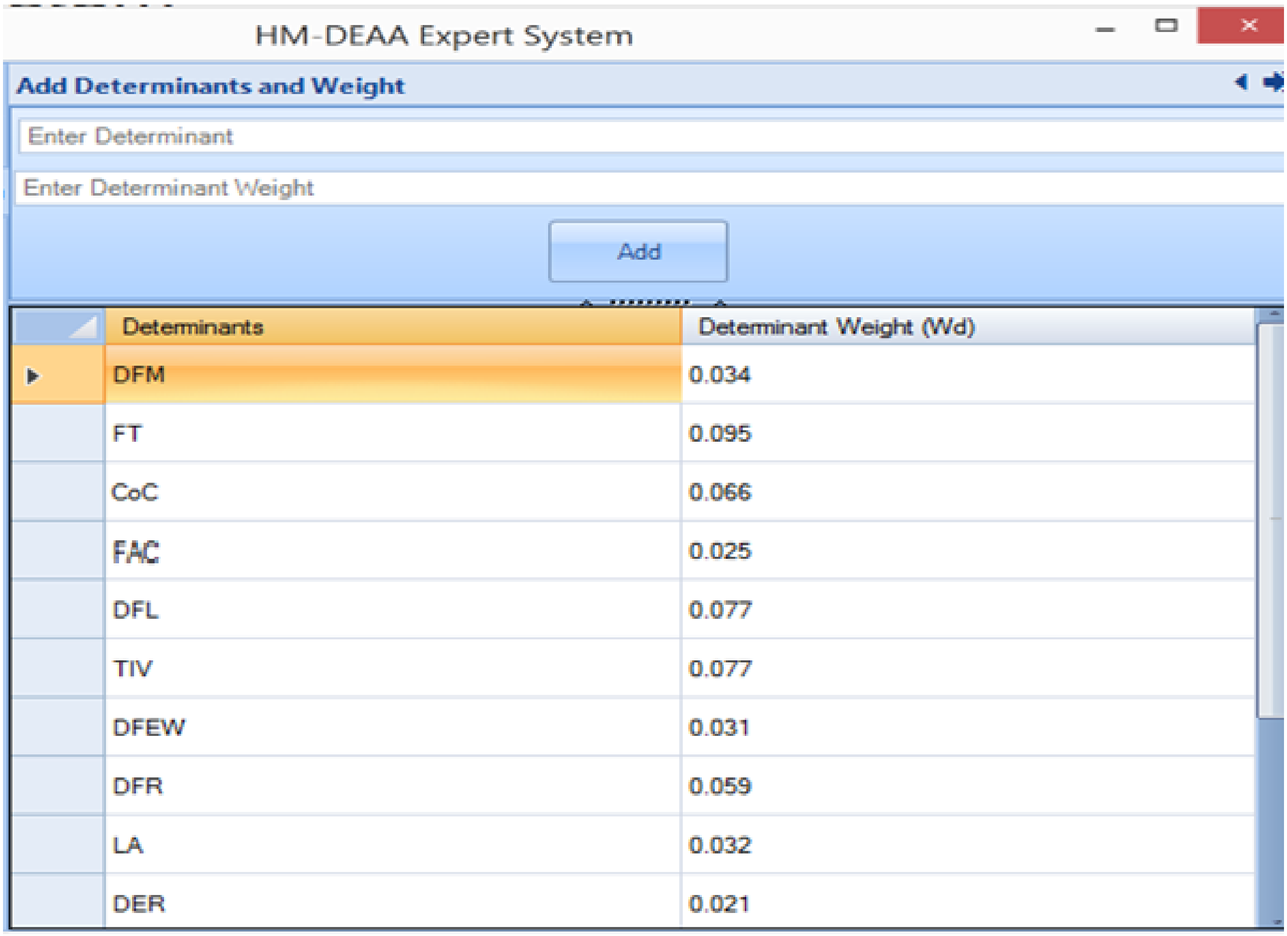
Table 8.1 HM-DEAA ExP Technical Requirements

HM-DEAA ExP Technical Requirements
The application requires at least Microsoft Windows 7, either x64 or x86
The operating system should have .Net Framework 4.0 installed.
The computer should have at least one web browser installed for viewing report.
The computer should have at least a memory of 512MB and a hard disk size of at least 20GB

The operational parameters of the HM-DEAA ExP are presented in the next section.

8.5. Operational Parameters for the HM-DEAA Expert System

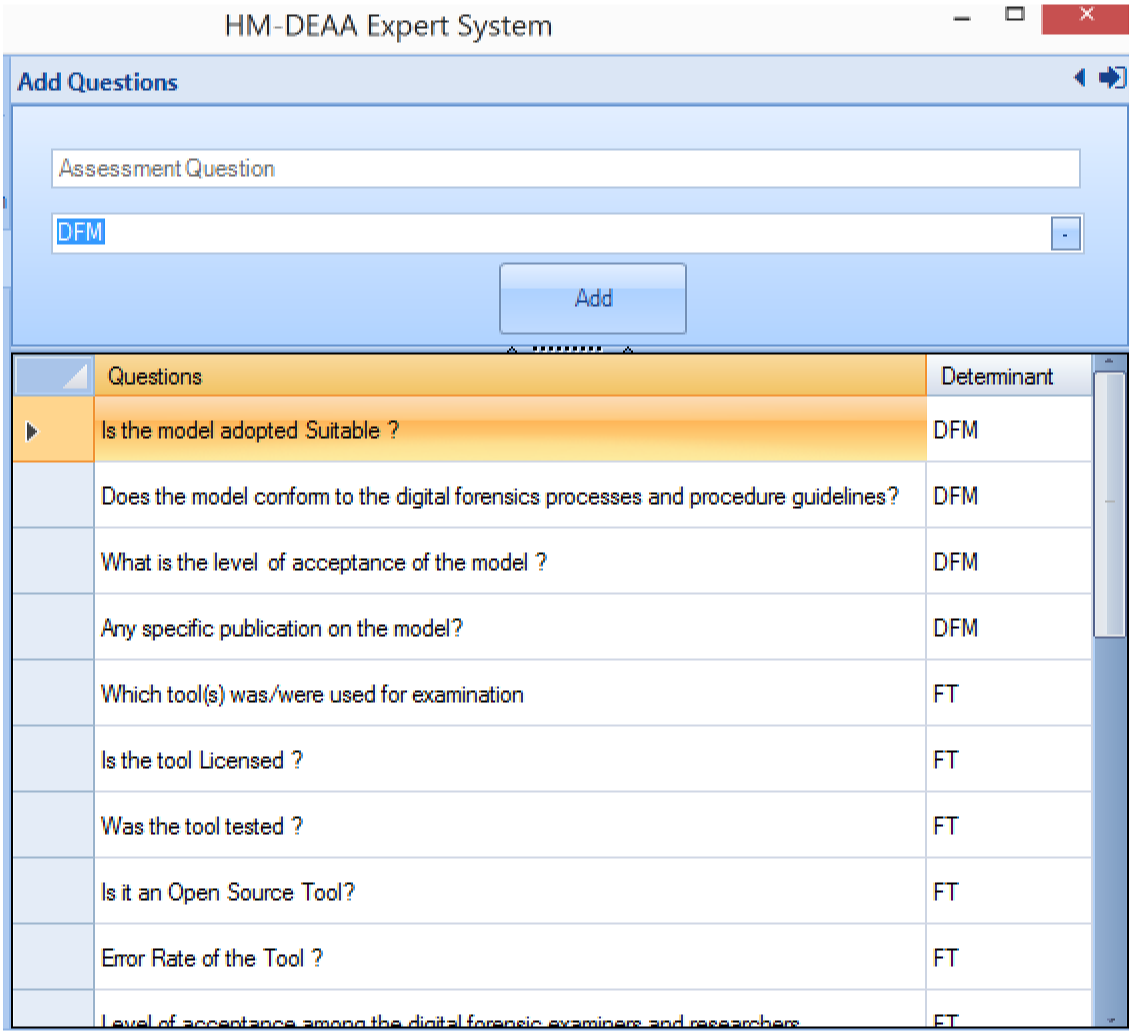
The HM-DEAA ExP uses the *Determinant Weights* obtained as presented in Chapter 6. A statistical tool such as Stata or SPSS is recommended to be used to obtain these values. Once the values are obtained, they are fed into the system for processing as evidenced in Figure 8.3. Either a judge with the required training or a technical assistant working with the courts can obtain these values as part of the setting up of the expert system.



Determinants	Determinant Weight (Wd)
DFM	0.034
FT	0.095
CoC	0.066
FAC	0.025
DFL	0.077
TIV	0.077
DFEW	0.031
DFR	0.059
LA	0.032
DER	0.021

Figure 8.3: Snapshot of HM-DEAA ExP showing the various Determinants and corresponding Weights

The system also requires the user to score each determinant based on the assessment questions and requirements. From the exploratory analysis involving the application of the HM-DEAA, the researcher has generated a list of assessment questions or requirements for each of the determinants as presented in Appendix F. Figure 8.4 highlights a number of assessment questions for the various determinants.



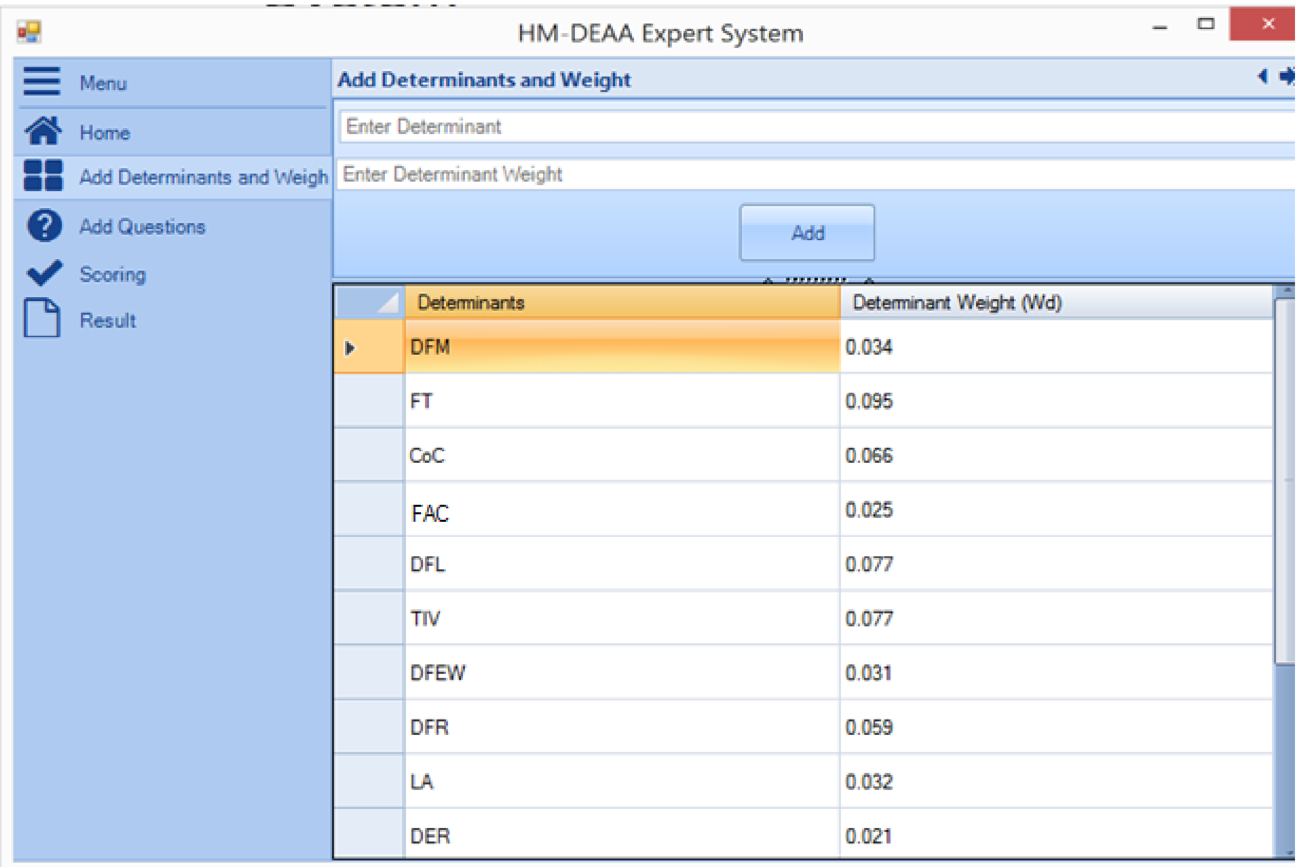
	Questions	Determinant
▶	Is the model adopted Suitable ?	DFM
	Does the model conform to the digital forensics processes and procedure guidelines?	DFM
	What is the level of acceptance of the model ?	DFM
	Any specific publication on the model?	DFM
	Which tool(s) was/were used for examination	FT
	Is the tool Licensed ?	FT
	Was the tool tested ?	FT
	Is it an Open Source Tool?	FT
	Error Rate of the Tool ?	FT
	Level of acceptance among the digital forensic examiners and researchers	FT

Figure 8.4: Snapshot of HM-DEAA ExP showing Assessment Questions of the Determinants

The HM-DEAA ExP allows multiple assessment questions for each determinant. In order to generate a *Determinant Score,* equation 7.6 in Chapter 7 is applied. This allows for an unlimited number of assessment questions by judicial authorities based on relevant technical and legal factors being considered for each determinant. The assessment questions in Appendix F are therefore not exhaustive.

8.6. Deployment and Evaluation of the HM-DEAA Expert System

The HM-DEAA ExP can either be installed from a removable drive or it can be deployed through a centralised server where users can easily install it from a Uniform Resource Locator (URL), which points to the application. To operate the system, a registered user must logon to the system using a username and password. Once that is done, the main interface of the application is presented to the user as highlighted in Figure 8.5.



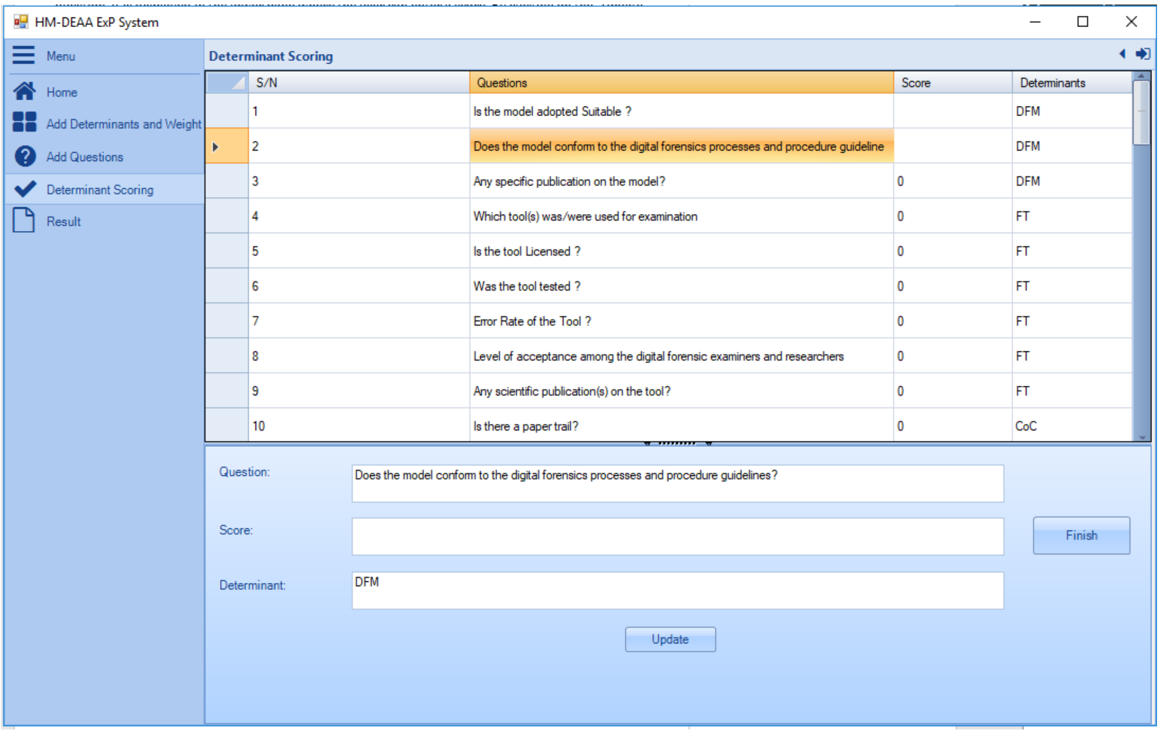
Determinants	Determinant Weight (Wd)
DFM	0.034
FT	0.095
CoC	0.066
FAC	0.025
DFL	0.077
TIV	0.077
DFEW	0.031
DFR	0.059
LA	0.032
DER	0.021

Figure 8.5: Main Interface of the HM-DEAA ExP Software

The user must enter the determinants and corresponding weights obtained during the Factor Analysis. The weight must be computed using a separate statistical tool as already explained. From Figure 8.5, it can be noted that the weight of each determinant has been entered into the system. After the determinants are entered into the system, the user is required to enter the assessment questions, as shown in Appendix F, for each determinant. These questions will later be used to score the evidence.

The HM-DEAA ExP system is designed to allow a user to add additional determinants and to generate *Determinant Scores* for each determinant before calculating evidential weight. In addition, the system can be customised for a particular jurisdiction by way of either removing, renaming or adding additional determinants. It is important to emphasize that *Determinant Weights* for the determinants can be modified based on new or updated research data (i.e., for each determinant weight in the HM-DEAA ExP system, the values can be modified by the user). For example, should a different survey be conducted in a particular jurisdiction and the survey results in different responses that can alter the existing values for the *Determinant Weights* obtained through the FA, the new values (i.e., values obtained for *Determinant Weights* from the new survey) can be inputted into the HM-DEAA ExP system before computing the *Determinant Scores.*

The determinants scoring tab of the software displays the assessment questions for the various determinants. The user can click on any of the questions to allocate a score. Once a user clicks on a question, it is displayed in the lower pane where the user can enter a score. By clicking on the "Update" button, the question selected is updated with the score allocated. The user can click on the "Finish" button after scoring all the assessment questions as evidenced in Figure 8.6.



S/N	Questions	Score	Determinants
1	Is the model adopted Suitable ?		DFM
2	Does the model conform to the digital forensics processes and procedure guideline		DFM
3	Any specific publication on the model?	0	DFM
4	Which tool(s) was/were used for examination	0	FT
5	Is the tool Licensed ?	0	FT
6	Was the tool tested ?	0	FT
7	Error Rate of the Tool ?	0	FT
8	Level of acceptance among the digital forensic examiners and researchers	0	FT
9	Any scientific publication(s) on the tool?	0	FT
10	Is there a paper trail?	0	CoC

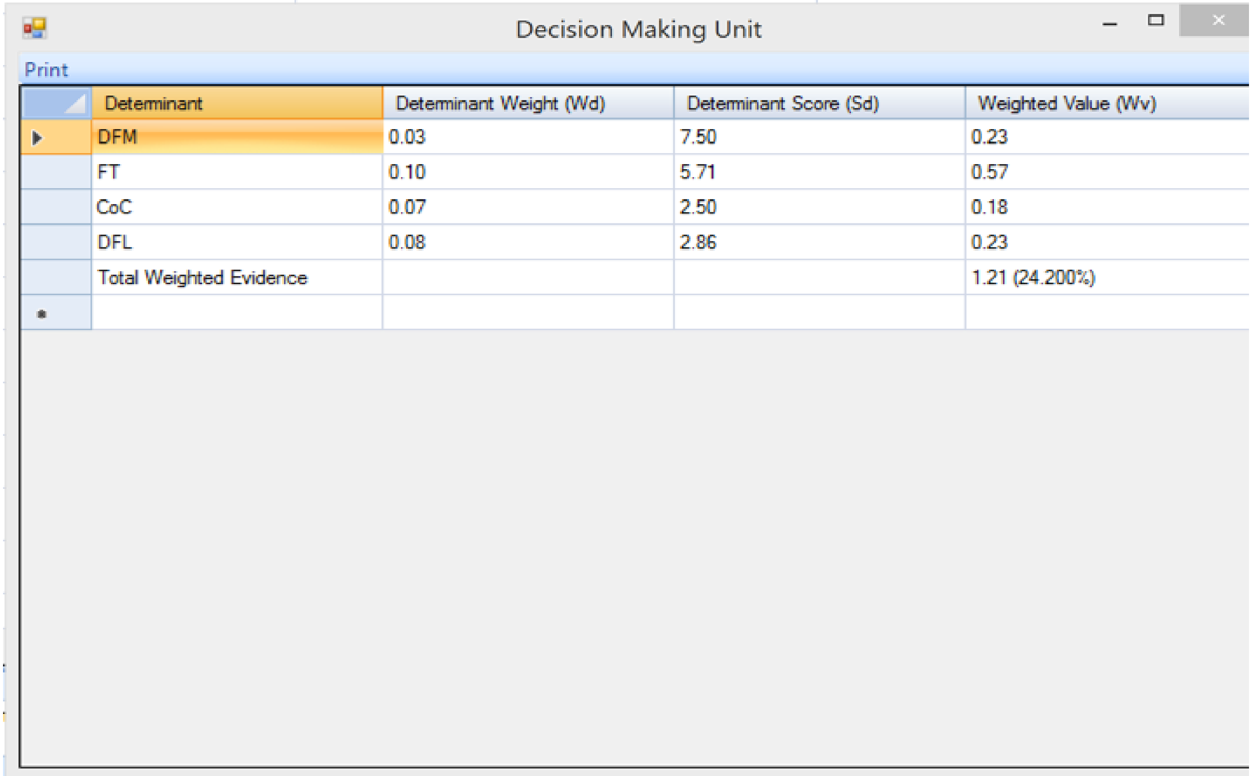
Question: Does the model conform to the digital forensics processes and procedure guidelines?

Score:

Determinant: DFM

Figure 8.6: HM-DEAA ExP Determinant Scoring

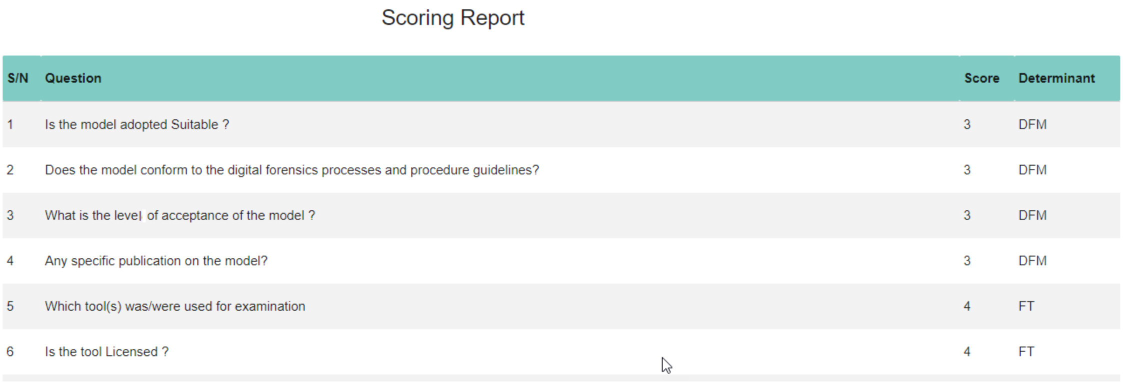
Once the user clicks the “Finish” button, the “Decision Making Unit” computes the *Evidential Weight* of the evidence assessed. Figure 8.7 highlights the *Total Evidential Weight*.



Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Weighted Value (Wv)
DFM	0.03	7.50	0.23
FT	0.10	5.71	0.57
CoC	0.07	2.50	0.18
DFL	0.08	2.86	0.23
Total Weighted Evidence			1.21 (24.200%)

Figure 8.7: Operations of the Decision-Making Unit of the HM-DEAA ExP

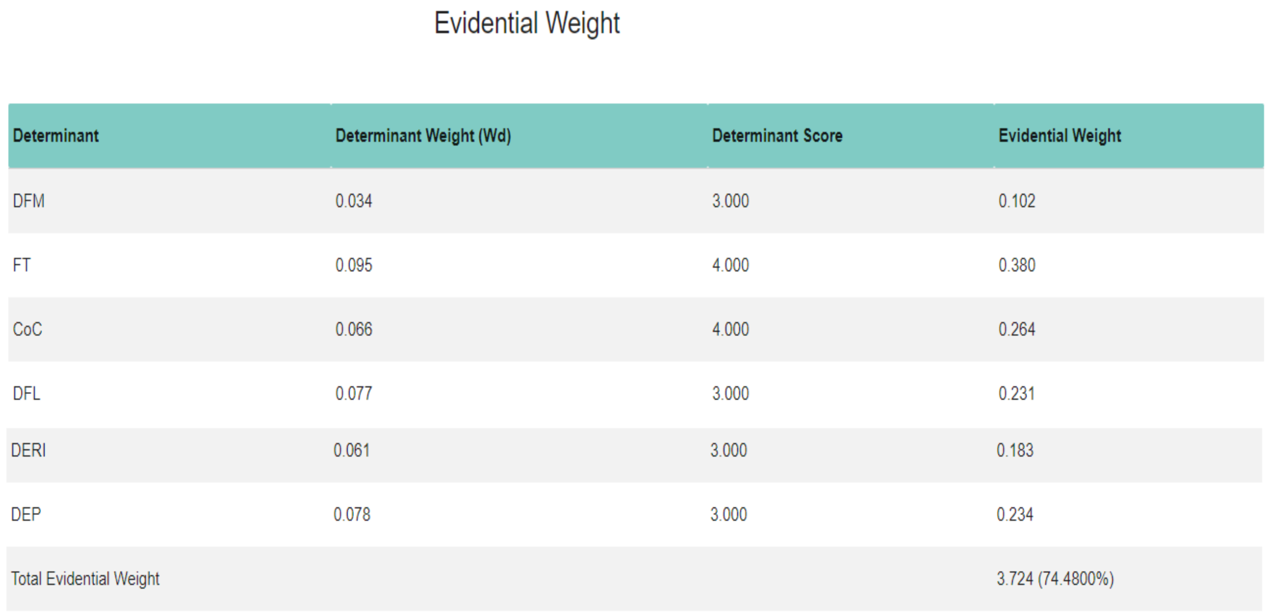
The user can generate a report by clicking on the “Print” button. An HTML report, as shown in Figure 8.8, is generated, which shows the various determinants considered, the various assessment questions scored, and the evidential weight generated. As a forensic application, a third party such as a higher court can conduct a review of the case and assess the scoring for the various determinants.



Scoring Report

S/N	Question	Score	Determinant
1	Is the model adopted Suitable ?	3	DFM
2	Does the model conform to the digital forensics processes and procedure guidelines?	3	DFM
3	What is the level of acceptance of the model ?	3	DFM
4	Any specific publication on the model?	3	DFM
5	Which tool(s) was/were used for examination	4	FT
6	Is the tool Licensed ?	4	FT

Figure 8.8: Snapshot of Scoring Report



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	4.000	0.380
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.724 (74.4800%)

Figure 8.9: Snapshot of Evidential Weight Report generated by the HM-DEAA ExP

The researcher has conducted an evaluation of the HM-DEAA through practical application of the system to 10 judicial cases. Details of the evaluation are presented in Chapter 9.

8.7. Conclusion

This chapter has presented the HM-DEAA ExP as a judicial tool. The scope of the application of the HM-DEAA ExP has been demonstrated and the practical application of the software to the criminal justice sector has been explained through the case scenario presented. This chapter has also discussed the requirements of the HM-DEAA ExP as well as the parameters to operationalise the application. Most importantly, the ability to customise the HM-DEAA ExP for a specific jurisdiction and its agility to meet potential legal and technological changes (i.e., ability to update the data such as values for *Determinant Weights* in the HM-DEAA ExP based on any changes in law or technology and render the expert system still relevant in its application in judicial proceedings) has been explained and demonstrated. Key considerations for the deployment of the HM-DEAA ExP have been presented and evaluation processes for implementing the tool has been discussed.

The next chapter discusses the application of the HM-DEAA with a specific focus on judicial case studies.

CHAPTER 9: APPLICATION OF HM-DEAA EXPERT SYSTEM (HM-DEAA ExP)

9.1. Introduction

The purpose of the Harmonised Model for Digital Evidence Admissibility Assessment Expert System (HM-DEAA ExP) is to practically assist judicial authorities to evaluate digital evidence for the purposes of administering criminal justice. The principal application of the tool is to assist judges to assess the *fit for purposeness* of digital evidence and to guide the process of establishing evidential weight of a given digital evidence. Consequently, having developed the HM-DEAA ExP, the researcher decided to test the software on cases that have already been adjudicated by the courts. This chapter discusses the application of the HM-DEAA ExP to real cases through direct engagement with the judges who adjudicated the cases considered for the case studies. For the purposes of this research, all the cases are anonymised.

The remainder of this chapter is constructed as follows. Section 9.2 discusses the application of the HM-DEAA ExP to 10 specific cases considered from Ghana's judiciary. The section discusses the application of the tool by judges as well as the tool's potential use by investigators, prosecutors and defence lawyers. Section 9.3 concludes this chapter with a summary of findings from the application of the HM-DEAA ExP.

9.2. Application of the HM-DEAA Expert System in Judicial Decision Making

The researcher conducted case study analysis covering the application of the HM-DEAA model to judicial cases. Ghana was selected for this case study because of the researcher's easy access to cases involving digital evidence and the availability of judges to engage with the researcher to discuss the application of the model to cases. The researcher has also been involved in a number of judicial matters involving digital evidence in Ghana and was therefore very familiar with application of the law to matters pertaining to digital evidence. In addition, as a government advisor, the researcher intends to implement findings from the research in Ghana's judiciary and therefore the case study was deemed necessary to ascertain the readiness of the judiciary to implement the HM-DEAA model.

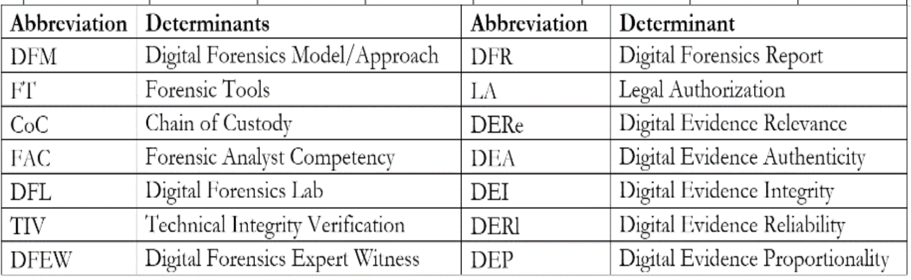
A questionnaire was sent to the judges involved for their initial review. This was followed by face-to-face discussions. The discussions with the selected judges focused on the application of the HM-DEAA model to criminal cases that have already been adjudicated. The researcher adopted this approach because it was initially realised that some of the judges may not fully comprehend the significance of the determinants and therefore could not provide valid responses to the questions. This approach is also underpinned by research findings that judges' understanding of technology and digital forensics processes significantly affect their understanding and consequently their decisions on cases involving digital evidence [64], [24], [67]. The researcher, therefore, met each of the judges and explained the rationale behind the case studies, which required them to review previous cases and provide their responses. Each of the judges who were involved in the study provided responses pertaining to the specific cases they presided over in their courts. Some of the judges had already participated in the research survey and therefore readily understood the requirements and the relevance of the case study.

Appendix H is the questionnaire administered for the case study. For each of the determinants, the judges were first asked to identify the assessment criteria and questions. The judges were further requested to allocate scores to each of the determinants. The score represents the value assigned to each of the determinants by the judges. The scores were computed using equation 7.6.

The various assessment questions used by the judges to score the determinants are provided in Appendix F. The scoring scale adopted ranges from 1 to 5, where 1 represents the lowest score (i.e. the assessment question met the lowest judicial requirements) and 5 represents the highest score (i.e. the assessment question met the highest judicial requirements). Detailed explanations on the scoring are provided in Appendix H, Guidance Note A. To ensure the judges understood the meaning and judicial significance of the various determinants, especially the technical determinants, the researcher explained to them the principles underlying the scoring before they completed the questionnaire. Table 9.1 presents a summary of findings pertaining to the scoring of the determinants.

Table 9.1: Case Responses

	Cases									
Determinants	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
DFM	4	4	3	3	1	3	3	2	3	-
FT	3	3	3	3	1	4	3	3	3	-
CoC	3	4	3	4	2	4	4	4	4	2
FAC	4	4	3	3	1	3	3	3	3	1
DFL	-	4	3	3	-	3	2	2	2	1
TIV	4	4	3	4	1	4	4	4	3	1
DFEW	4	5	-	-	-	5	-	-	-	-
DFR	4	4	4	3	1	4	4	3	3	1
LA	3	4	3	3	3	3	3	4	5	3
DER	4	4	4	4	2	4	4	3	3	3
DEA	3	3	3	4	2	4	3	3	4	2
DEI	3	3	3	3	2	4	4	3	3	1
DERl	3	4	3	3	1	3	4	4	4	1
DEP	3	3	3	4	2	3	4	3	3	-



Abbreviation	Determinants	Abbreviation	Determinant
DFM	Digital Forensics Model/Approach	DFR	Digital Forensics Report
FT	Forensic Tools	LA	Legal Authorization
CoC	Chain of Custody	DERe	Digital Evidence Relevance
FAC	Forensic Analyst Competency	DEA	Digital Evidence Authenticity
DFL	Digital Forensics Lab	DEI	Digital Evidence Integrity
TIV	Technical Integrity Verification	DERl	Digital Evidence Reliability
DFEW	Digital Forensics Expert Witness	DEP	Digital Evidence Proportionality

Table 9.1 depicts the various scores given by the judges for the determinants across the 10 cases considered. From Table 9.1, the judge who presided over Case 1 allocated a score of 4 to DFM determinant. The same judge allocated a score of 3 to DEI determinant. According to the judge, she could not recall whether the digital evidence involved in the case, which she adjudicated in 2016, was processed in a standard digital forensics laboratory. The judge further indicated that though forensic lab is important in ensuring quality assurance, its absence in this case did not affect the case overall, as key requirements such as the FAC and DER were met. In addition, the expert witness who testified in the case was able to "enlighten" the court on key questions raised by both the prosecution and the defence.

In Case 10, the judge who adjudicated the case indicated that the forensic report submitted did not make any reference to the forensic approach adopted and the forensic tool used so she could not provide a score. It was further revealed that the prosecutors could not make any arguments in reference to or in support of both the DFM and the FT. In addition, the judge indicated that because no external expert witness was involved, he could not provide any score for that particular determinant.

Appendix F highlights the various assessment criteria and questions identified by the judges who participated in the exploratory analysis. Some of the judges referred to both literature and legal precedents in identifying the assessment questions. Apart from scoring each of the determinants in the cases, the researcher also discussed the nature of the cases adjudicated, the typology of digital evidence involved, the criminal offences applied in each of the cases, sentencing guidelines and requirements, and other relevant judicial considerations, which could impact on judicial decisions.

The analysis of the responses from the judges as presented above correlates to a fact which has been established in this study: judicial decisions on digital evidence are essentially impacted by the knowledge and understanding of both the technical and legal determinants, and their application in the judicial processes. With particular reference to Ghana, judges' understanding of matters pertaining to digital evidence is generally limited, even though a small number of judges, especially those who preside on cases at the commercial courts, have an excellent understanding of digital evidence and the application of both procedural and substantive laws relative to digital evidence.

Furthermore, the inability of both the prosecution and defence to make any legal arguments or raise any technical issues relative to DFM and FT in Case 10 also suggests that both the prosecutions and the defence had limited knowledge and understanding of issues pertaining to digital evidence as is normally the case in practice. Indeed, the judge confirmed that both the prosecutor and the lead defence counsel were ill-equipped with knowledge and understanding of digital evidence and its application in the Ghanaian criminal justice system.

Upon the application of the HM-DEAA on the *Determinant Scores* provided by the judges through the exploratory analysis, the following results obtained pertaining to evidential weight for each of the cases are shown in Table 9.2.

Table 9.2: Evidential Weight from the Exploratory Analysis of 10 Judicial Cases

S/N	Case ID/Reference	Evidential Weight Generated (%) Using HM-DEAA
1	Case 1	60.32%
2	Case 2	70.28%
3	Case 3	59.74%
4	Case 4	65.70%
5	Case 5	29.30%
6	Case 6	74.48%
7	Case 7	68.00%
8	Case 8	60.64%
9	Case 9	63.14%
10	Case 10	21.40%

From Table 9.2, suspects who were involved in all, but case 5 and case 10 were convicted of the various criminal charges for which they were tried for by the courts. Relative to both cases where *Evidential Weights* calculated using the HM-DEAA were below 30%, suspects were acquitted because according to the judges, the overall evidence presented which comprised significant components of digital evidence did not meet the burden of evidential proof required for convictions under the offences for which the suspects were arraigned before the courts. Further details of the above interpretation are presented in this chapter.

To illustrate the application of the HM-DEAA on the cases reviewed, the researcher adopted both the manual application and the expert system in the 10 cases. The manual application is based on equation 7.9 which was presented in Chapter 7. The expert system is the automation of the processes and activities to generate the evidential weight, which is represented by the HM-DEAA ExP. The objective for adopting both the manual application and the expert system was to validate the operationalisation of the HM-DEAA model using both the manual and automated systems in order to see how closely the expert system performed to the manual application. It should be noted that the manual application is assumed to be completely correct. The application of the manual application and the expert system to Case 1, Case 6 and Case 10 are discussed further in this chapter. The researcher has chosen to present discussions involving the three cases since there is not enough space to discuss all 10 cases.

8.2.1. Manual Calculation: Case 1

For Case 1, the judge provided the following *Determinant Scores* as presented in Table 9.3.

Table 9.3: Case 1 Determinants' Scores

SN	Determinant	Assessment Score (1–5)
1	Digital Forensics Model	4
2	Forensic Tools	3
3	Chain of Custody	3
4	Forensic Analyst Competency	4
5	Digital Forensics Lab	-
6	Technical Integrity Verification	4
7	Digital Forensics Expert Witness	4
8	Digital Forensics Report	4
9	Legal Authorisation	3
10	Digital Evidence Relevance	4
11	Digital Evidence Authenticity	3
12	Digital Evidence Integrity	3
13	Digital Evidence Reliability	3
14	Digital Evidence Proportionality	3

The Evidential Weight for each determinant is determined with *equation 7.7* and the Total Evidential Weight is calculated with *equation 7.9.* The Total Evidential Weight is expressed as a percentage with *equation 7.10.*

Applying the mathematical formula to compute the Total Evidential Weight *equation 7.9* for Case 1 is as follows:

Evidential Weight (Ev) *= Determinant Weight (Wd) * Determinant Score (Sd)*

Total Evidential Weight =

$$\sum_{i=1}^{n} Wd_iSd_i = Wd_1Sd_1 + Wd_2Sd_2 + Wd_3Sd_3 + \cdots + Wd_nSd_n$$

=

(4*0.034)+(3*0.095)+(3*0.066)+(4*0.025)+(0*0.077)+(4*0.77)+(4*0.031)+(4*0.059)+

(3*0.032)+(4*0.021)+(3*0.136)+(3*0.208)+(3*0.061)+(3*0.078)

= 3.016

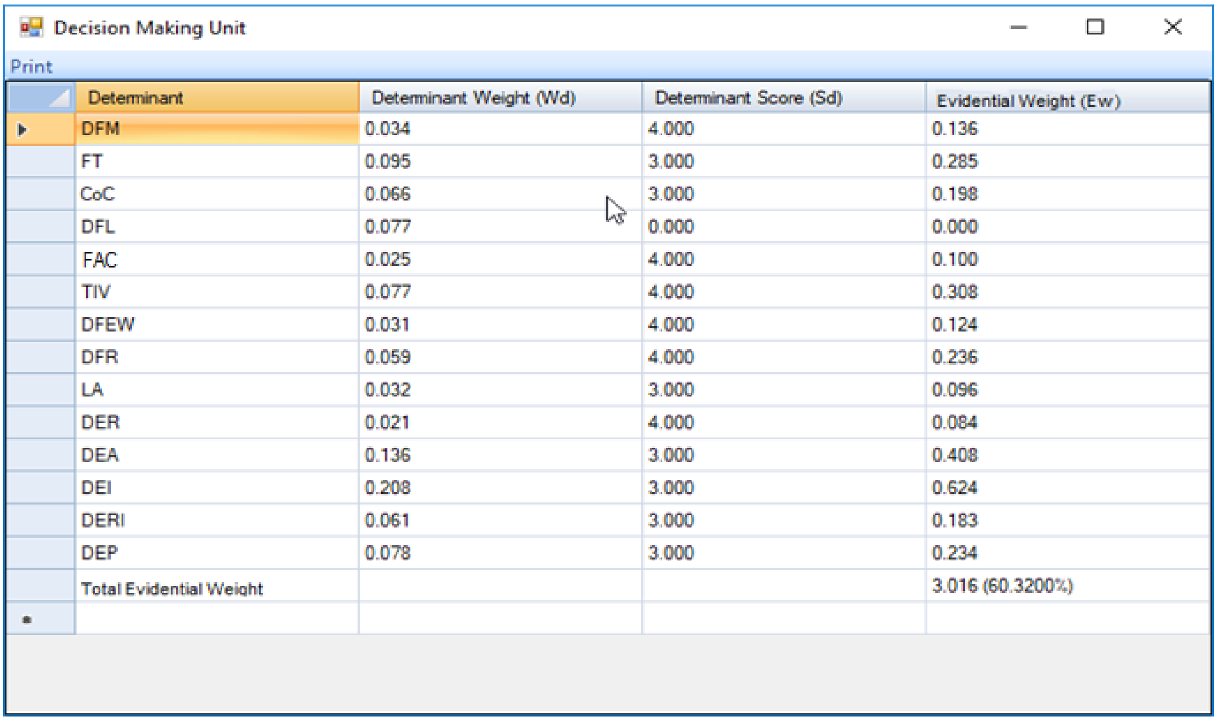
Expressing the Total Evidential Weight in percentage using Equation 7.10

$$\frac{EW}{5} * 100$$

$$\frac{3.016}{5} * 100\% = 60.32\%$$

9.2.2. Automated Calculation with HM-DEAA ExP System: Case 1

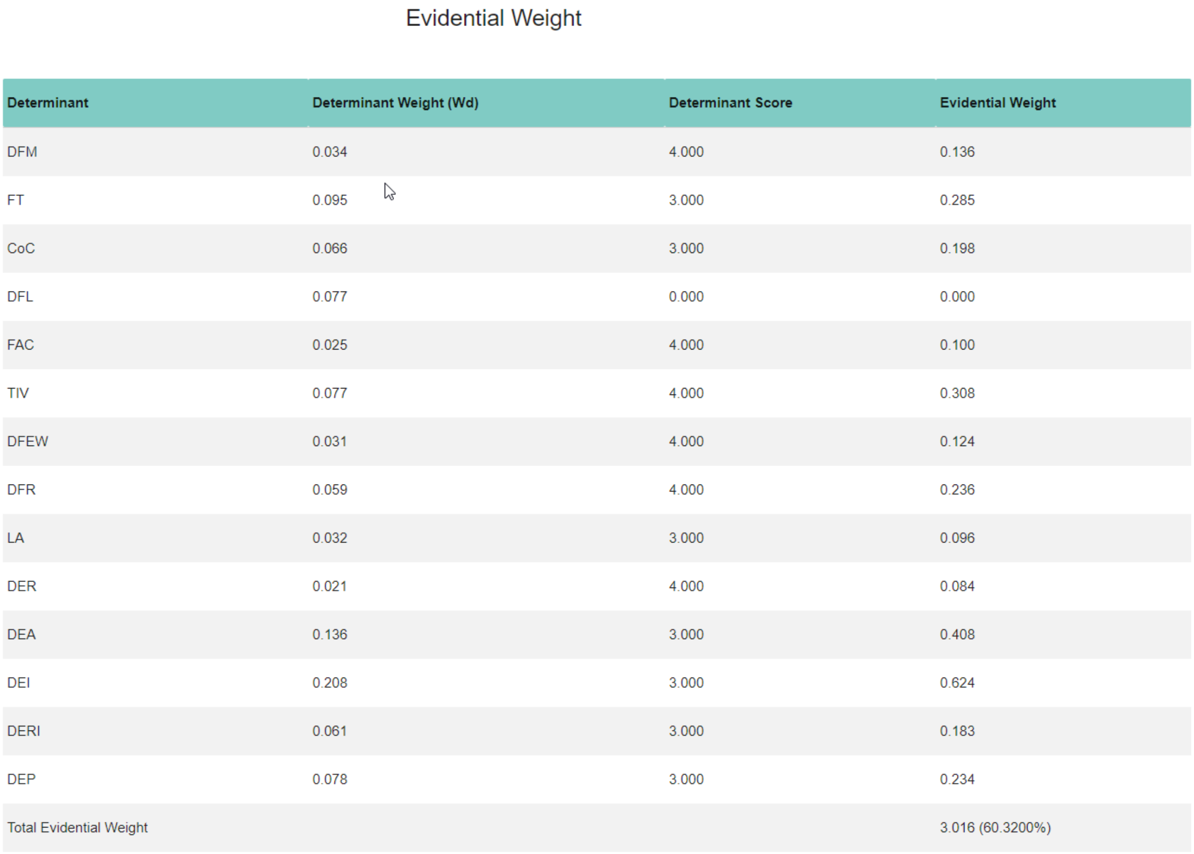
Using the HM-DEAA ExP, *Evidential Weight* for Case 1 is generated through the computation of *Determinant Weight* and *Determinant Score* as evidenced in Figure 9.1.



Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (Ew)
DFM	0.034	4.000	0.136
FT	0.095	3.000	0.285
CoC	0.066	3.000	0.198
DFL	0.077	0.000	0.000
FAC	0.025	4.000	0.100
TIV	0.077	4.000	0.308
DFEW	0.031	4.000	0.124
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.016 (60.3200%)

Figure 9.1: Determinant Weight for Case 1 using HM-DEAA ExP

A report from the HM-DEAA showing the Evidential Weight for Case 1 is generated using a web browser as shown in Figure 9.2.



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	4.000	0.136
FT	0.095	3.000	0.285
CoC	0.066	3.000	0.198
DFL	0.077	0.000	0.000
FAC	0.025	4.000	0.100
TIV	0.077	4.000	0.308
DFEW	0.031	4.000	0.124
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.016 (60.3200%)

Figure 9.2: Report on Case 1 from the HM-DEAA ExP

For Case 1, an evidential weight of 60.32% was generated when the HM-DEAA was applied to the *Determinants Scores* provided by the judge during the exploratory analysis of Case 1. According to the details from the analysis, the judge sentenced the suspect to 4 years for *Defrauding by False Pretense* under Section 131 (1) of the Criminal Offences Act, 1960 (Act 29) [122] and Section 123 of the Electronic Transactions Act, 2008 (Act 772) of the Republic of Ghana. The judge considered the sentence as average (as opposed to minimum or maximum sentence) and indicated that a number of mitigating factors were taken into consideration before the sentence. He cited the length of time that the suspect had spent in custody during the trial as one of the mitigating factors considered in sentencing the suspect for the crime in question, which would otherwise have attracted a minimum of 10 years' imprisonment.

9.2.3. Manual Calculation: Case 6

For Case 6, the judge provided the following *Determinants Scores* as shown in Table 9.4.

Table 9.4: Case 6 Determinants' Scores

SN	Determinant	Assessment Score (1–5)
1	Digital Forensics Model	3
2	Forensic Tools	4
3	Chain of Custody	4
4	Forensic Analyst Competency	3
5	Digital Forensics Lab	3
6	Technical Integrity Verification	4
7	Digital Forensics Expert Witness	5
8	Digital Forensics Report	4
9	Legal Authorisation	3
10	Digital Evidence Relevance	4
11	Digital Evidence Authenticity	4
12	Digital Evidence Integrity	4
13	Digital Evidence Reliability	3
14	Digital Evidence Proportionality	3

The *Evidential Weight* for each determinant is determined with *equation 7.7* and the Total Evidential Weight is calculated with *equation 7.9.* The Total Evidential Weight is expressed as a percentage with *equation 7.10.*

Applying the mathematical formula to compute the Total Evidential Weight *equation 7.9* for Case 6 is as follows:

Total Evidential Weight =

$$\sum_{i=1}^{n} Wd_i Sd_i = Wd_1 Sd_1 + Wd_2 Sd_2 + Wd_3 Sd_3 + \cdots + Wd_n Sd_n$$

=

(3*0.034)+(4*0.095)+(4*0.066)+(3*0.025)+(3*0.077)+(4*0.77)+(5*0.031)+(4*0.059)+

(3*0.032)+(4*0.021)+(4*0.136)+(4*0.208)+(3*0.061)+(3*0.078)

= 3.756

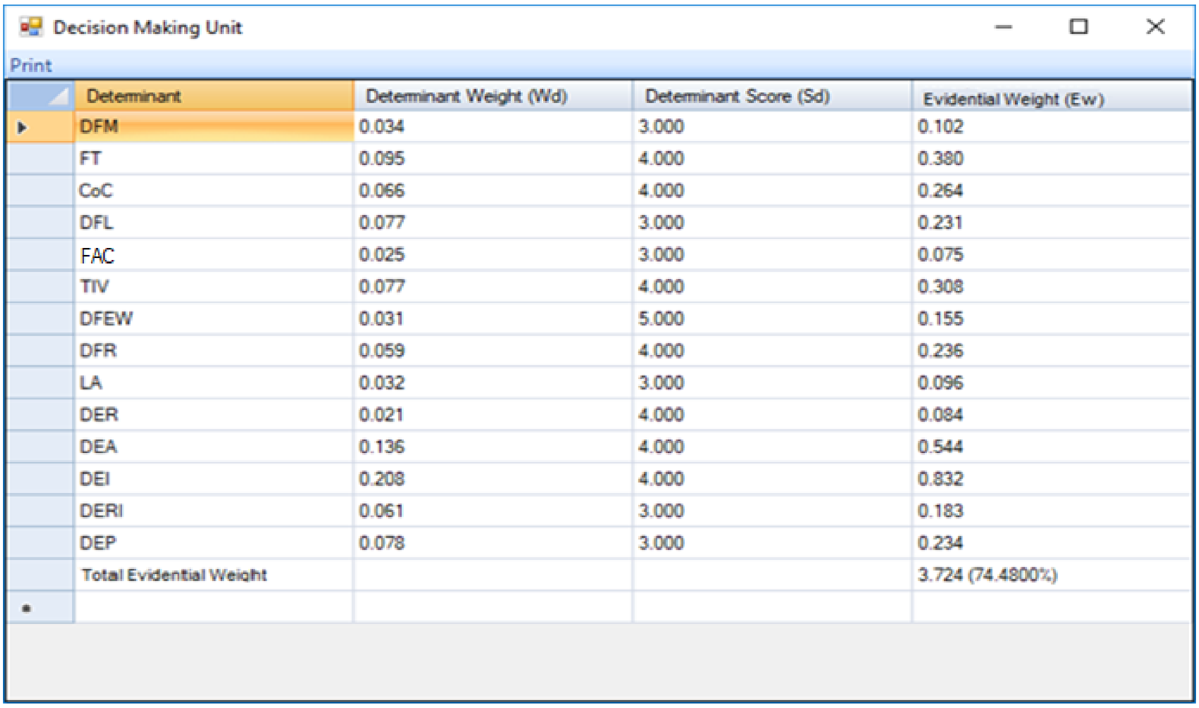
Expressing the Total Evidential Weight in percentage using Equation 7.10

$$\frac{EW}{5} * 100$$

$$\frac{3.724}{5} * 100\% = 74.48\%$$

9.2.4. Automated Calculation with HM-DEAA ExP System: Case 6

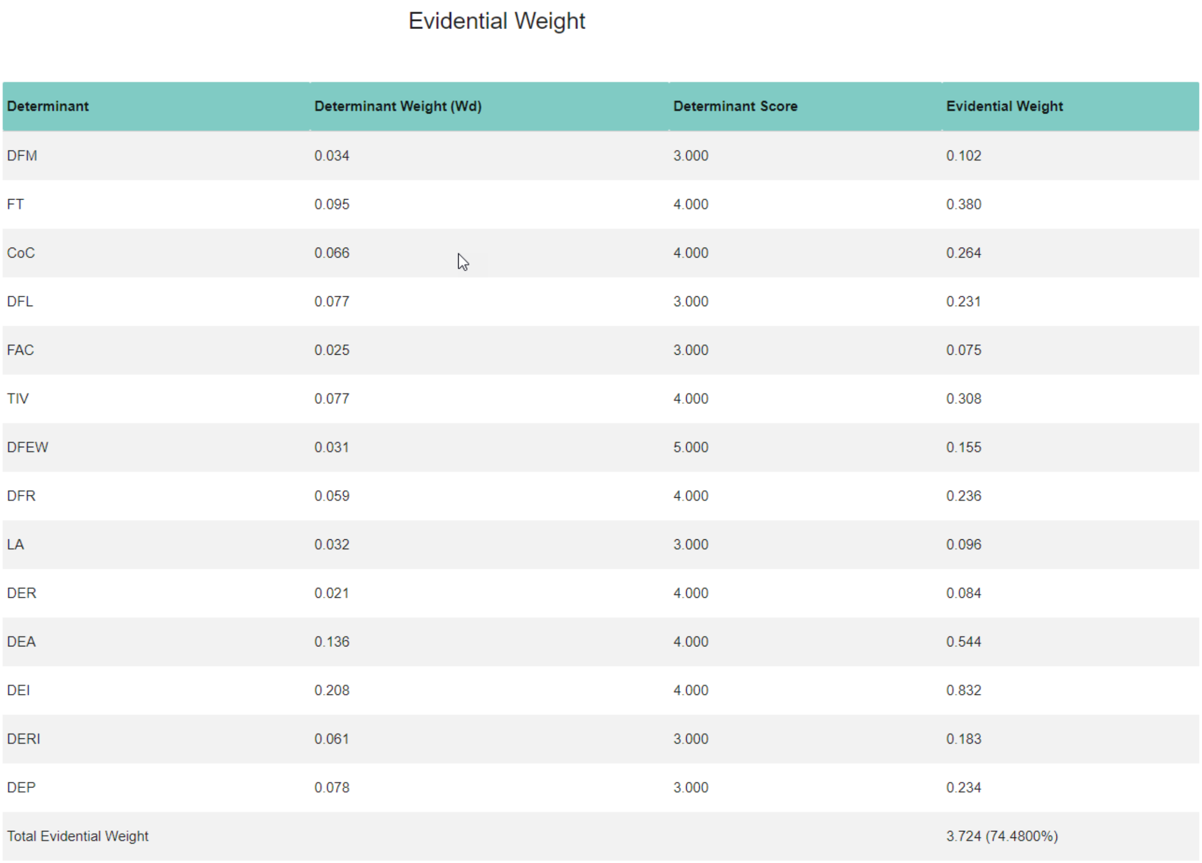
Using the HM-DEAA ExP, *Evidential Weight* for Case 6 is generated through the computation of *Determinant Weight* and *Determinant Score* as evidenced in Figure 9.3.



Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (Ew)
DFM	0.034	3.000	0.102
FT	0.095	4.000	0.380
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	5.000	0.155
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	4.000	0.544
DEI	0.208	4.000	0.832
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.724 (74.4800%)

Figure 9.3: Determinant Weight for Case 6 using HM-DEAA ExP

A report from the HM-DEAA showing the Evidential Weight for Case 6 is generated using a web browser, as shown in Figure 9.4.



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	4.000	0.380
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	5.000	0.155
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	4.000	0.544
DEI	0.208	4.000	0.832
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.724 (74.4800%)

Figure 9.4: Report on Case 6 from the HM-DEAA ExP

On Case 6, the judge explained that it involved illegal interception and interference of international calls usually called SIM box fraud.[8] The accused was charged with providing *Electronic Communication Service without Authority* contrary to 73(1)(c) of the Electronic Communications Act, 2008 (Act 775),[9] and *Possessing Illegal Device* contrary to section 135 of the Electronic Transactions Act, 2008 (Act 772). Upon the evaluation of the digital evidence produced during the trial, the accused was sentenced to a term of imprisonment of 24 months in addition to payment of 2000

[8] A Subscriber Identity Module (SIM) box fraud is a fraudulent setup in which perpetrators install SIM boxes with multiple low-cost prepaid SIM cards. The fraudster then can terminate international calls through local phone numbers in the respective country to make it appear as if the call is a local call. https://www.telekom-icss.com/newsroom/news/news-pages/151638

[9] The Electronic Communications Act, 2008 (Act 775) is an Act of Ghanaian Parliament, which provides for the regulation of electronic communications, the regulation of broadcasting, the use of the electromagnetic spectrum and for related matters. https://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf

penalty units.[10] According to the judge, a breach of section 73 (1) of Act 769 carries a fine of not more 3000 penalty units, a term of imprisonment of not more than five years or both.

Considering the maximum sentence under the law, the judge deemed the sentence for the accused as "above average". However, he also indicated that he considered one mitigating factor — the fact that the accused had operated the illegal SIM box business for only 6 months as confirmed by forensic evidence contrary to what the prosecutors wanted the court to believe.

9.2.5. Manual Calculation: Case 10

The judge who adjudicated the case provided the following *Determinants Scores* as presented in Table 9.5.

[10] Penalty unit is an amount of money used to compute pecuniary penalties for many breaches of statute law. In Ghana, 1 penalty unit is equivalent to about USD 2.5.

Table 9.5: Case 10 Determinants' Scores

SN	Determinant	Assessment Score (1–5)
1	Digital Forensics Model	-
2	Forensic Tools	-
3	Chain of Custody	2
4	Forensic Analyst Competency	1
5	Digital Forensics Lab	1
6	Technical Integrity Verification	1
7	Digital Forensics Expert Witness	-
8	Digital Forensics Report	1
9	Legal Authorisation	3
10	Digital Evidence Relevance	3
11	Digital Evidence Authenticity	2
12	Digital Evidence Integrity	1
13	Digital Evidence Reliability	1
14	Digital Evidence Proportionality	-

The *Evidential Weight* for each determinant is determined with *equation 7.7* and the Total Evidential Weight is calculated with *equation 7.9.* The Total Evidential Weight is expressed as a percentage with *equation 7.10.*

Applying the mathematical formula to compute the Total Evidential Weight *equation 7.9* for Case 10 is as follows:

Total Evidential Weight =

$$\sum_{i=1}^{n} Wd_i Sd_i = Wd_1 Sd_1 + Wd_2 Sd_2 + Wd_3 Sd_3 + \cdots + Wd_n Sd_n$$

=

(0*0.034)+(0*0.095)+(2*0.066)+(1*0.025)+(1*0.077)+(1*0.77)+(0*0.031)+(1*0.059)+

(3*0.032)+(3*0.021)+(2*0.136)+(1*0.208)+(1*0.061)+(0*0.078)

= 1.07

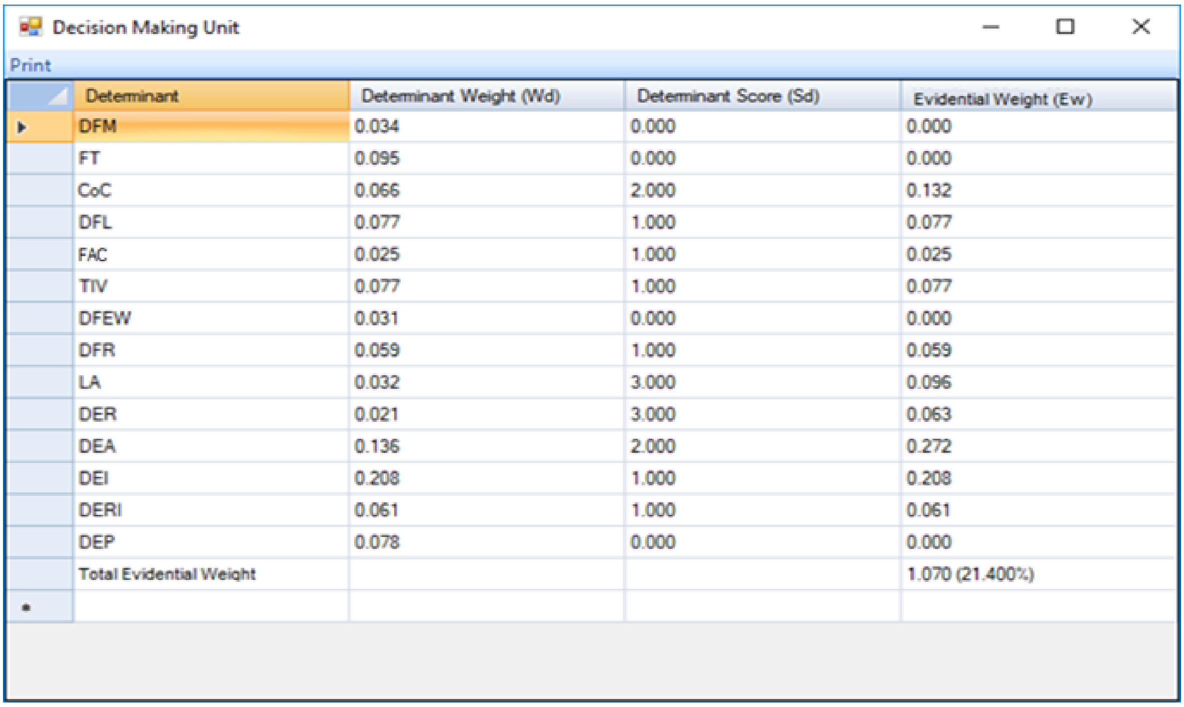
Expressing the Total Evidential Weight in percentage using Equation 7.10

$$\frac{EW}{5} * 100$$

$$\frac{1.07}{5} * 100\% = 21.4\%$$

9.2.6. Automated Calculation with HM-DEAA ExP System: Case 10

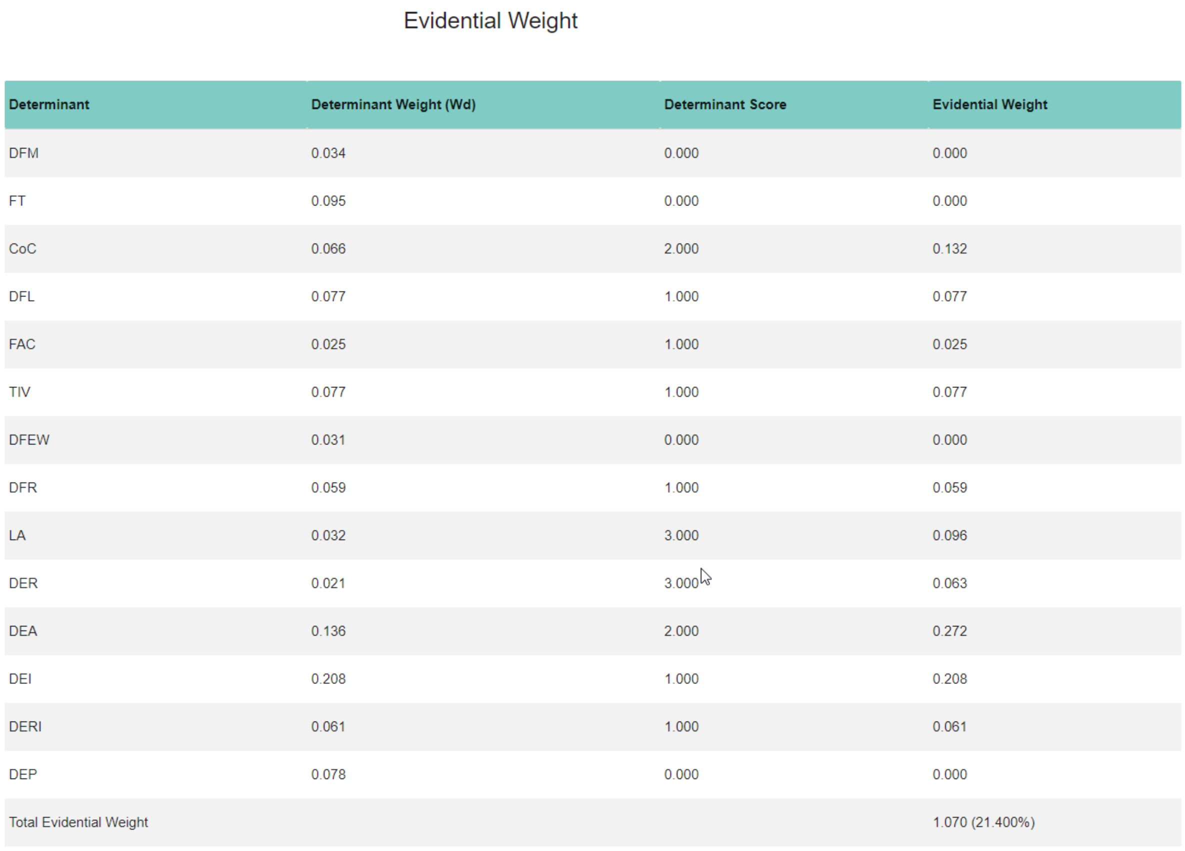
Using the HM-DEAA ExP, *Evidential Weight* for Case 10 is generated through the computation of *Determinant Weight* and *Determinant Score* as evidenced in Figure 9.5.



Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (Ew)
DFM	0.034	0.000	0.000
FT	0.095	0.000	0.000
CoC	0.066	2.000	0.132
DFL	0.077	1.000	0.077
FAC	0.025	1.000	0.025
TIV	0.077	1.000	0.077
DFEW	0.031	0.000	0.000
DFR	0.059	1.000	0.059
LA	0.032	3.000	0.096
DER	0.021	3.000	0.063
DEA	0.136	2.000	0.272
DEI	0.208	1.000	0.208
DERI	0.061	1.000	0.061
DEP	0.078	0.000	0.000
Total Evidential Weight			1.070 (21.400%)

Figure 9.5: Determinant Weight for Case 10 using HM-DEAA ExP

A report from the HM-DEAA ExP showing the Evidential Weight for Case 10 is generated using a web browser as shown in Figure 9.6.



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	0.000	0.000
FT	0.095	0.000	0.000
CoC	0.066	2.000	0.132
DFL	0.077	1.000	0.077
FAC	0.025	1.000	0.025
TIV	0.077	1.000	0.077
DFEW	0.031	0.000	0.000
DFR	0.059	1.000	0.059
LA	0.032	3.000	0.096
DER	0.021	3.000	0.063
DEA	0.136	2.000	0.272
DEI	0.208	1.000	0.208
DERI	0.061	1.000	0.061
DEP	0.078	0.000	0.000
Total Evidential Weight			1.070 (21.400%)

Figure 9.6: Report on Case 10 from the HM-DEAA ExP

With Case 10, the suspect was acquitted as the prosecution could not provide any relevant and reliable digital evidence to support the charges.

Table 9.2 provides a picture of the Evidential Weights for each of the cases considered as part of the case studies. The nexus between the Evidential Weight and the sentences given by the judges has been established within a certain percentage range. For example, in Case 10, the judge acquitted the suspect because the determinants considered did not meet the overall required threshold overall for sentencing. It is also important to emphasize that judges have some discretionary powers under the law that they exercise when they deem it necessary. According to the judges who participated in the case studies, a number of mitigating factors are usually taken into consideration when delivering a judgement. These factors include the age of the accused, guilty plea, number of years already spent in custody, demonstration of remorse and other extenuating factors. In addition, O'Brien et. al. [102] have raised some shortfalls pertaining to the application of forensic science in criminal justice. The efficiency of the delivery of justice system especially in developing countries, the admissibility of expert evidence in criminal proceedings, the believability of reliability tests as well as possible bias and influence of legal representations are specific external constraints that could impact on the success of HM-DEAA's application in judicial proceedings.

The existence of these extra-scientific factors in addition to the discretionary powers of judges as far as judicial decisions are concerned does not undermine the scope of HM-DEAA model in providing a scientific basis for a judicial decision. Thus, the HM-DEAA is used to assess the case and to help establish the scientific basis for sentencing. Mitigating factors are considered after the HM-DEAA has provided the judge in question with the required scientific guidance to make a judicial decision. It is therefore appropriate to indicate that the scope of application of the HM-DEAA is scientific in nature while acknowledging that other non-scientific factors, as explained above, could impact final judicial decisions. Mitigating factors and the discretionary powers allotted to judges as arbiters of justice do not therefore affect the *scientificity* of the HM-DEAA as a judicial tool.

It is also important to note that despite the established correlation between the findings from the application of the HM-DEAA tool and the outcome of the 10 cases explored, the HM-DEAA should not be seen only as a confirmatory judicial tool. Operationally, the HM-DEAA is designed to proactively support the judicial process in assessing digital evidence admissibility and providing a rational basis for evidential weight determination before a case is adjudicated. Most importantly, the HM-DEAA tool can help resolve a potential judicial dispute involving lower and upper courts. For example, the HM-DEAA tool can be deployed to assess a case, which is being challenged in the upper court, by assisting to either confirm an earlier judgement by a lower court or by providing different indicators that will lead to a different judicial decision.

The application of the HM-DEAA model is operationally relevant to other criminal justice practitioners too. Considering the assessment criteria and questions provided by the judges, investigators, prosecutors and defence lawyers can equally use the same questions to evaluate the potential use of digital evidence in a court of law. This underlines the wider scope of HM-DEAA's application in the criminal justice sector as highlighted in the scenario presented in Chapter 8. The next section concludes this chapter with an emphasis on the scope and application of the HM-DEAA model.

9.3. Conclusion

Findings from the case study have confirmed the foundation of the HM-DEAA ExP as a judicial tool. The application of the HM-DEAA ExP to specific cases has also revealed a significant research finding — the fact that other extenuating circumstances and factors such as mitigating factors based on a country's specific sentencing guidelines could impact on the final decision in a case involving digital evidence. The classic judicial statement, "temper justice with mercy" [123], which is normally prayed by defence in pleading leniency for suspects, further highlights the fluidity associated with judicial decisions beyond the scientific evidence. Mitigating factors and discretionary powers are well grounded in legal philosophy and criminal law. Therefore, in order for the HM-DEAA model to take its rightful place in judicial proceedings, it has to take cognizance of these extenuating judicial considerations.

It is therefore important to emphasize that the purpose and the scope of HM-DEAA ExP as a system to support judicial decision making is based on proven scientific evidence, which is underpinned by both technical and legal determinants. In other words, the theory and practice of resolving the *techno-legal dilemma* which is the object of this research is scientifically driven with expected scientific outputs. The HM-DEAA ExP thus becomes a scientific judicial tool, which can be utilised in any jurisdiction to support the criminal justice sector in the process of investigating, prosecuting and most importantly, adjudicating cases involving digital evidence.

PART 5: EVALUATION

Part Five of the thesis focuses on evaluation of the research. In the context of this thesis, the term evaluation refers to the assessment of the merits and demerits of the research. This part consists only of the evaluation chapter, Chapter 10. This chapter discusses the main contributions of the research especially in the area of digital forensics standardisation. This chapter also critically evaluates the drawbacks of the research and proposed future works in the area.

CHAPTER 10: EVALUATION

10.1. Introduction

The research goal of the thesis was to resolve the *techno-legal dilemma,* which was introduced as the research problem, at two levels: first, to establish the foundation of digital evidence admissibility in judicial proceedings and second, to establish the foundation and a system for the determination of the evidential weight of digital evidence. In order to achieve the objectives of the research, the researcher identified the various technical and legal determinants of digital evidence admissibility. A survey was conducted to validate the determinants introduced. The Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) was developed based on the technical and legal determinants established through the research. The research further introduced an algorithm upon which a formula was generated to calculate the evidential weight of digital evidence. An expert system, which is underpinned by the HM-DEAA model, was introduced to operationalise the model as a judicial tool applicable in criminal justice proceedings. As part of research evaluation, the model has been tested on real judicial cases.

This chapter critically evaluates the research. The remainder of this chapter is constructed as follows. Section 10.2 discusses the thesis' contribution to research especially in the area of digital forensics standardisation. Section 10.3 discusses the research's drawbacks as well as specific considerations for future work in the area. Section 10.4 concludes this chapter with a summary.

10.2. Key Research Contributions

Chapter 2.5 of the thesis traces the historical development of digital forensics standardisation. The literature review presented suggests that different efforts have been made by researchers and practitioners towards rationalizing the domain of digital forensics as a forensic science. The focus of this research was to address issues relative to the admissibility of digital evidence in legal proceedings. The research has established an interdependent relationship between technical and legal determinants. In other words, each of the technical and legal determinants impact each other in order to support scientific judicial conclusions. As a result of this finding, it has been established that a judge's decision on matters pertaining to digital evidence is based on both technical and legal determinants. The research has therefore established the scientific foundations of digital evidence admissibility in legal proceedings.

In addition, the application of science to law for the purpose of justice is significantly important and therefore such matters cannot be handled in an ad-hoc manner. The relevance of a harmonised approach towards digital evidence admissibility as the basis for standardisation is further strengthened by the need for international cooperation on cybercrime investigations and prosecutions. Cybercrime is borderless and the standardisation of the application of digital forensics processes and procedures across different jurisdictions is essential for effective judicial cooperation across borders.

As a main contribution to the wider research in the area of digital forensics, the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) has introduced a solution that provides a holistic foundation and a framework for the judicial assessment of digital evidence. Whilst models presented in Section 2,5 are fundamentally *investigations-oriented*, the HM-DEAA is *judicial proceedings-oriented*. As a result, the HM-DEAA as a new model is complementary to existing models. The HM-DEAA therefore extends digital forensics standardization efforts beyond investigations to practical judicial proceedings where the focus of judicial actors is on digital evidence — its admissibility and evidential weight. As evidenced by the application of the HM-DEAA to real cases, the model has further rationalised the judicial approach to establishing digital evidence admissibility and determining evidential weight. As a result, the introduction of the HM-DEAA is significantly important both in research and in practice. Apart from the model's contribution to digital forensics standardisation, the HM-DEAA has been introduced as a judicial tool to facilitate the work of the courts in matters pertaining to digital evidence.

The introduction of the HM-DEAA is therefore the novel contribution of the thesis towards digital forensics standardisation and the development of digital forensics as a scientific discipline.

10.3. Research Drawbacks and Future Work

The HM-DEAA model proposed has addressed the key research questions outlined in Chapter 1. The concluding chapter details the findings of this research and how these findings address the research questions raised. However, the researcher recognises some key limitations associated with the model, which can be improved through future research:

1. The field of digital forensics continues to evolve in view of emerging developments in ICT. Since the HM-DEAA is significantly underpinned by technological realities, these anticipated developments in digital forensics are expected to impact on the model proposed. Future research is therefore recommended to identify any other technical and legal determinants that may

emerge as important areas for consideration in digital evidence admissibility assessment. The agility of the HM-DEAA makes it possible for additional integration of both technical and legal determinants.

2. The research has produced a *Determinant Assessment Toolkit (DAT)*. The DAT is expected to serve as an important resource and reference for judges in implementing the HM-DEAA. Further research is recommended to identify additional factors, which judicial officials could consider in assessing each determinant's score in establishing evidential weight of digital evidence. Thus, regular updates of the DAT through research is recommended.

3. The researcher believes that developments in the field of digital forensics could impact on the data generated from the survey to compute the *Determinants' Weights* through the application of the Factor Analysis (FA). The researcher is conscious that the survey conducted to obtain the foundation for the FA analysis was carried out at a certain point in time and therefore its validity is limited to a specific timeframe. In the interest of future research, regular validation of the determinants as well as the information that constitutes the basis for the determination of the weights for the determinants is significantly important to ensure the relevance of the HM-DEAA model for continuous use by judges.

4. The HM-DEAA ExP requires an external statistical tool to compute the weights of the individual determinants, which will allow for the user assessment to produce the determinant scores. This constitute a technical drawback relative to the independence of the expert system to operate its functions. Further

work is required to incorporate relevant statistical and analysis tools based on the FA requirements into the HM-DEAA ExP to ensure the tool does not rely on external applications or systems to operate.

5. In addition, the validity of the proposed model is essentially dependent on the level of technical knowledge and legal understanding of judicial actors in the application of the HM-DEAA model to judicial proceedings. Digital forensics is still in a state of development and a number of judicial systems have not yet developed the required maturity in knowledge and understanding of the rudiments of digital evidence and its application in judicial matters. Legal reforms and judicial training on digital evidence is expected to improve the application of the HM-DEAA as a functional model for digital evidence admissibility assessment in legal proceedings.

6. For future research, practical application of the HM-DEAA in different jurisdictions including cases adjudicated by juries is recommended to ensure its continuous validation as a reproducible model that is operationally relevant in different legal contexts.

10.4. Conclusion

This chapter has presented the research evaluation. The contributions of the proposed HM-DEAA model to digital forensics research and practice have been duly presented and discussed herein. The introduction of the HM-DEAA as a foundation of digital evidence admissibility assessment and the application of the model in judicial proceedings together comprise the study’s main contribution to digital forensics research and practice.

This chapter has also presented specific drawbacks associated with the research and its potential implications on the model introduced. The researcher has provided research suggestions and operational recommendations towards improving the functional goal of the HM-DEAA model in particular and digital forensics standardisation in general.

PART 6: CONCLUSION

Part Six of the thesis focuses on the conclusions of the research. This part consists of a single chapter; Chapter 11. This chapter revisits the introductory part of the research by establishing the nexus between the research questions raised and findings from this study. This chapter explains how the research has addressed the problem statement and the specific research questions underpinning the study.

CHAPTER 11: CONCLUSION

11.1. Introduction

This thesis represented the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA), a model to assess digital evidence admissibility in judicial proceedings. This chapter provides the conclusion to the thesis. This chapter revisits the problem statement introduced in chapter 1 and discusses the research findings as well as the impacts of these findings on digital evidence admissibility. Section 11.3 concludes this chapter with a summary.

11.2. Revisiting the Problem Statement and Research Implications

The aim of the research was to make measurable contributions to current efforts aimed at digital forensics standardisation. To achieve this goal, the researcher identified an important problematic area upon which a problem statement for the thesis was formulated. Despite the progressive efforts and successes in the domain of digital forensics standardisation, the question of digital evidence admissibility in judicial proceedings remained one of the key issues arising from the application of digital forensics in criminal justice administration. While existing literature and legislations have identified a number of approaches and requirements pertaining to the application of digital evidence in criminal legal proceedings, the rationalization of the various determinants and the dilemma around the functional interactions among both the various determinants were unresolved, hence the basis for introducing the *techno-legal dilemma* as the research theme.

In addition, even though different countries have introduced a number of cyber-related legislations and knowledge gaps relative to the application of digital forensics processes and techniques are being addressed through training and capacity building programmes for the judiciary, a holistic model to serve as a framework to guide judicial authorities in establishing an appropriate foundation of digital evidence admissibility had not been introduced prior to this thesis.

In establishing the techno-legal foundation of digital evidence admissibility, which was the goal in resolving the *techno-legal dilemma*, the researcher formulated this problem statement: *What reproducible and standardised framework integrates both technical and legal determinants to establish the admissibility of digital evidence in legal proceedings?* The thesis has answered this research question by introducing the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA), which was presented in Chapter 5.

The HM-DEAA has been introduced to rationalise and standardise digital evidence admissibility applicable in judicial proceedings. The model provides a holistic foundation to establish digital evidence admissibility because it integrates both the technical and legal determinants into a single process model, which can also be operationalised in judicial proceedings. The research has established that the technical and legal determinants, which underpin digital evidence admissibility are trans-jurisdictional in nature and this effectively establishes the reproducibility of the HM-DEAA model as a common standard for digital evidence admissibility assessment across different legal jurisdictions.

In order to address the problem statement introduced in the thesis, the research raised a number of sub-research questions, which have been addressed by the study.

1. *What technical determinants underpin the admissibility of digital evidence?* The objective of this research question was to identify the various technical

determinants that underpin digital evidence admissibility. Chapter 4 of the study has addressed this question by identifying the various determinants, namely digital forensics model determinant, digital forensics tool determinant, chain of custody determinant, forensic analyst competency determinant, digital forensics laboratory determinant, technical integrity verification determinant, digital forensics expert witness determinant and digital forensics report determinant. These determinants are validated through the survey, which are presented in Chapter 6. These technical determinants are trans-jurisdictional in nature as they are applicable across different jurisdictions.

2. *What legal determinants underpin the admissibility of digital evidence?* Another objective of the research was to identify specific legal determinants, which constitutes the legal foundation of digital evidence admissibility. Chapter 4 has identified legal authorisation, digital evidence relevance, digital evidence authenticity, digital evidence integrity, digital evidence reliability and digital evidence proportionality as the main legal determinants of digital evidence admissibility. These determinants were validated through the same survey involving judicial actors. The research has established that the application of law in the criminal justice sector, irrespective of the crime typology and the jurisdiction of its application, has unique protocols that constitute the legal determinants of digital evidence admissibility.

3. *What is the relationship between technical and legal determinants in establishing the admissibility of digital evidence?* In establishing the foundations of a harmonised model to determine admissibility of digital evidence, one of the objectives identified for this study was to determine the kind of relationship

between the technical and legal determinants in providing the basis for digital evidence admissibility. The *techno-legal dilemma* presupposes that there are some expectations around the interactions between both the technical and the legal determinants in order to provide an integrated foundation for digital evidence admissibility. The research has established an interdependent relationship between the technical and legal determinants. The HM-DEAA framework as represented in Chapter 5 highlights this interdependent relationship. The output of the interactions among technical and legal determinants constitute the basis of digital evidence admissibility. To further demonstrate this interdependency, the researcher introduced an algorithm to illustrate the logical sequences of the relationship between the various determinants as presented in Chapter 7. The application of Factor Analysis (FA) to data generated from the survey has further established a correlation between the technical and legal determinants as explained in Chapter 7. This research has therefore established that judicial decisions on matters pertaining to digital evidence are based on the interactions of both the technical and the legal determinants.

4. *What are the determinants of evidential weight of a piece of digital evidence?* The research also sought to investigate the foundations of evidential weight of digital evidence. In other words, this study sought to identify the factors that determine the weight that a judge will normally attach to a particular piece of digital evidence, which is tendered in court. The research has established that each of the determinants has some bearing not only on digital evidence admissibility but also in determining the evidential weight of evidence admitted. Thus, each technical

and legal determinant has its unique impact on the collective weight that a judge will assign to the digital evidence in question.

Findings from the case study involving the application of the HM-DEAA to judicial cases as presented in Chapter 9 have provided perspectives into the factors that inform a judicial decision when digital evidence is being considered. The thesis has established that there are specific factors that underpin each of the determinants. These specific factors are the considerations for allocating a score to a particular determinant based on specific judicial requirements and assessment benchmarks. For example, in assigning a score to the digital forensics tool determinant, some specific questions including the following are taken into consideration:

- Which tool(s) was/were used for the forensic examination?
- Was/were the tool(s) licensed?
- Was/were the tool(s) tested/validated? By which body?
- Has/ve the tool(s) been previously used in a similar case in another court?
- Was/were the tool(s) open-source or proprietary?
- Any impact of the tool(s) used on the case?
- Any error rate of the tool(s)? Is the error rate known?
- What is the level of acceptance of the tool(s) among the digital forensic practitioners and researchers?
- Any scientific publication(s) on the tool?
- Other considerations.

Appendix F highlights the various assessment questions obtained from the case studies involving judicial cases, which are presented in Chapter 9. As a practical deliverable, this study has produced a *Determinant Assessment Toolkit (DAT)* which is expected to provide guidance to judges and other judicial actors in the application of the HM-DEAA in judicial proceedings.

5. *How is the evidential weight of digital evidence determined?* The HM-DEAA as a judicial tool is evaluated based on its practical application in judicial proceedings. An important objective of the research was to determine evidential weight of digital evidence given in a particular situation. In achieving the objective underlying this research question, the researcher expanded the scope of application of the HM-DEAA model by developing a framework for calculating the evidential weight of digital evidence using factor analysis (FA). The researcher adopted FA to construct the weights of the various determinants, which are required for judicial decisions. Data collated from the survey provided the theoretical framework to implement the FA. The researcher adopted *Pearson Correlation Coefficient* to establish a correlation between the technical and legal determinants upon which the FA was implemented. Chapter 7 explains the application of the FA in the determination of evidential weight of digital evidence.

   The researcher has evaluated the equation generated from the FA by applying the framework to real cases as presented in Chapter 9. One of the most significant outputs of this research is the development and implementation of a framework for calculating the evidential weight of digital evidence. As anticipated by the study, the framework introduced is reproducible as its application can be customised for a specific legal jurisdiction.

The HM-DEAA has been introduced to resolve the *techno-legal dilemma* by introducing a framework that operationally harmonises both the technical and the legal determinants of admissibility. In addition, the HM-DEAA has been introduced to address the question of evidential weight determination in judicial proceedings. The next section concludes this chapter with a summary.

11.3. Conclusion

This chapter has presented the concluding narrative of the research project. This chapter revisited the theme for the research by identifying the key research questions framing this study. The researcher has presented a summary of research findings in relation to the research questions underlying this study. This chapter has therefore presented and discussed the findings, which address the specific research questions raised as part of the thesis' concluding narrative.

BIBLIOGRAPHY

[1] S. Goodison, R. Davis and B. Jackson, Digital Evidence and the US Criminal Justice System: Identifying Technology and other Needs to more Effectively Acquire and Utilize Digital Evidence, Santa Monica, Califonia: RAND, 2015.

[2] INTERPOL, "Crime Areas: INTERPOL," [Online]. Available: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. [Accessed 2018].

[3] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Waltham, Massachusetts: Academic Press, 2011.

[4] Digital Forensics Research Workshop (DFRWS), "A Roadmap for Digital Forensic Research," in *Proceedings of The Digital Forensic Research Conference*, Utica, New York, 2001.

[5] M. Reith, C. Carr and G. Gunsch, "An Examination of Digital Forensics Models," *International Journal of Digital Evidence,* vol. 1, no. 3, 2002.

[6] A. Valjarevic and H. Venter, "Harmonised Digital Forensic Investigation Process Model," in *Proceedings of the Information Security for South Africa Conference*, Johannesburg, Gauteng, South Africa, 2012.

[7] Association of Chief Police Officers, Good Practice Guide for Computer-Based Evidence, London, United Kingdom, 2008.

[8] The U.S Department of Justice , Electronic Crime Scene Investigation - A Guide for First Responders, Washington, D.C; USA: National Institute of Justice, 2001.

[9] International Organization for Standardization, "Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," ISO/IEC 27037:2012 Standard, Geneva, Switzerland, 2012.

[10] International Organization for Standardization, Information Technology - Security Techniques - Incident Investigations Principles & Processes, ISO/IEC 27043:2015 Standard, Geneva, Switzerland, 2015.

[11] N. Eubanks, "The True Cost of Cybercrime for Businesses," Forbes, 2017. [Online]. Available: http://www.forbes.com/sites/theysec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/amp. [Accessed 2017].

[12] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Model," *Journal of Advances in Computer Networks,* vol. 3, no. 1, pp. 82-86, 2015.

[13] M. Abulaish and N. A. H. Haldar, "Advances in Digital Forensics Frameworks and Tools: A Comparative Insight and Ranking," *International Journal of Digital Crime and Forensics,* vol. 10, no. 2, pp. 95-119, 2018.

[14] M. Pollitt, "Computer Forensics: An Approach to Evidence in Cyberspace," in *18th Natonal Information Systems Security Conference*, Baltimore, Maryland, USA, 1995.

[15] M. Pollitt, "Applying Traditional Forensic Taxonomy to Digital Forensics," in *Advances in Digital Forensics IV, International Federation for Information Processing*, New York, USA, Springer Science+Business Media, LLC, pp. 17-26, 2008.

[16] M. Grobler, "Digital Forensic Standards: International Progress," in *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)* , Port Elizabeth, South Africa, 2010.

[17] Council of Europe, "Electronic Evidence Guide," 2013.

[18] American Academy of Forensic Sciences, "Proceeding: American Academy of Forensic Sciences," in *68th Annual Scientific Meeting*, Las Vegas, Nevada, 2016.

[19] Shorter Oxford English Dictionary, 6 ed., Oxford University Press,, 2007.

[20] R. Saferstein, Forensic Science: From the Crime Scene to the Lab, Pearson Prentice Hall, 2009.

[21] L. Gottschalk, J. Liu, B. Datham, S. Fitzgerald and M. Stein, "Computer Forensics Programs in Higher Education: A Preliminary Study," *ACM SIGCSE Bulletin,* vol. 37 , no. 1, pp. 147-151, 2005.

[22] K. Kuchta, "Computer Forensics Today," *Information Systems Security,* vol. 9, no. 1, pp. 1-5, 2000.

[23] G. Palmer, "A Road Map for Digital Forensic Research - Report from the First Digital Forensic Research Workshop, DFRWS Technical Report, DTR-T001-01 FINAL," Air Force Research Laboratory, Rome, 2001.

[24] F. Cohen, Digital Forensic Evidence Examination, Livermore, Califonia: ASP Press, 2010.

[25] J. Jordaan, "Ensuring the Legality of the Digital Forensics," *International Journal of Computer Applications,* vol. 68, no. 23, 2013.

[26] C. Grobler and B. Louwrens, Digital Forensics: A Multi-Dimensional Discipline, Publication of ISSA, Research Paper, 2006.

[27] K. Inman and N. Rudin, Principles and Practice of Criminalistics : The Profession of Forensic Science, Boca Raton, Florida: CRC Press, 2001.

[28] F. Alanazi and A. Jones , "The Value of Metadata in Digital Forensics," in *2015 European Intelligence and Security Informatics Conference*, Manchester, UK, 2015.

[29] H. Arshed, A. Jantan and O. Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *Journal of Information Processing Systems,* vol. 14, pp. 346 - 376, 2018.

[30] R. Leigland and A. Krings, "A Formalization of Digital Forensics," *International Journal of Digital Evidence,* vol. 3, no. 2, 2004.

[31] V. R. Kebande, A Novel Cloud Forensic Readiness Service Model, pp 28, 2017.

[32] S. Zimmerman and D. Glavach, "Cyber Forensics in the Cloud," *IAnewsletter,* vol. 14, no. 1, pp. 4-7, 2011.

[33] Scientific Working Group on Digital Evidence, SWGDE Best Practices for Computer Forensics. Version 3.1, 2014.

[34] A. Agarwal, M. Gupta, S. Gupta and S. Gupta, "Systematic Digital Forensic Investigation Model.," *International Journal of Computer Science and Security (IJCSS),* vol. 5, no. 1, pp. 118 -131, 2011.

[35] S. Perumal, N. Norwawi and V. Raman, "Internet of Things (IoT) Digital Forensic Investigation Model: TopDown Forensic Approach Methodology," in *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC),* Switzerland , 2015.

[36] M. Harbawi and A. Verol, "An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework," in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)* , Tirgu Mures, Romania , 2017.

[37] B. Martini and K.-K. Choo, "An Integrated Conceptual Digital Forensic Framework for Cloud Computing.," *Digital Investigation,* vol. 9, no. 2, p. 71–80, 2012.

[38] A. M. Edington and R. Kishore, "Forensics framework for cloud computing," *Computers & Electrical Engineering,* vol. 60, pp. 193-205, 2017.

[39] S. K. A. Manoj and D. Bhaskari, "Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment," *Procedia Computer Science,* vol. 85, pp. 149-154, 2016.

[40] N. Ab Rahman, W. Glisson, Y. Yang and K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," *IEEE Cloud Computing,* vol. 3, no. 1, pp. 50-59, 2016.

[41] "Big Data and Digital Forensics," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* , Vancouver, BC, Canada , 2016.

[42] H. Mohammed, N. Clarke and F. Li, "An Automated Approach for Digital Forensic Analysis of Heterogeneous Big Data," *Journal of Digital Forensics, Security and Law ,* vol. 11, no. 2, 2016.

[43] B. Carrier and E. H. Spafford, "Getting Physical with the Digital Investigation Process," *International Journal of Digital Evidence,* vol. 2, no. 2, pp. 1-20., 2003.

[44] J. Tan, Forensic Readiness, Cambridge, MA: Stake Inc., 2001.

[45] R. Rowlingson, "A Ten Step Process for Forensic Readiness," *International Journal of Digital Evidence,* vol. 2, no. 3, 2004.

[46] N. H. Ab Rahman , . N. D. W. Cahyani and . K. R. Choo, "Cloud Incident Handling and Forensic-by-Design: Cloud Storage as a Case Study," *Concurrency and Computation: Practice and Experience. Published online 19 May 2016 in Wiley Online Library (wileyonlinelibrary.com). https://doi.org/10.1002/cpe.3868 ,* 2017.

[47] G. Grispos, W. B. Glisson and K.-K. R. Choo, "Medical Cyber-Physical Systems Development: A Forensics-Driven Approach," in *Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies*, Philadelphia, Pennsylvania, 2017.

[48] A. Alenezi, R. K. Hussein, R. J. Walters and G. B. Wills, "A Framework for Cloud Forensic Readiness in Organizations," in *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, San Francisco, CA, USA, 2017.

[49] D. Ras and H. Venter, "Proactive Digital Forensics in the Cloud using Virtual Machines," in *2015 International Conference on Computing, Communication and Security (ICCCS)*, Pamplemousses, Mauritius, 2015.

[50] G. Grispos, J. García-Galán, L. Pasquale and B. Nuseibeh, "Are You Ready? Towards the Engineering of Forensic-Ready Systems," in *11th IEEE International Conference on Research Challenges in Information Science*, Brighton, United Kingdom, 2017.

[51] L. Pasquale, D. Alrajeh, C. Peersman, T. Tun, B. Nuseibeh and A. Rashid, "Towards Forensic-Ready Software Systems," in *Proceedings of the 40th International Conference on Software Engineering: New Ideas and Emerging Results - ICSE-NIER '18*, Gothenburg, Sweden, 2018.

[52] M. Al Fahdi, . N. Clarke and S. Furnell , "Challenges to Digital Forensics: A Survey of Researchers & Practitioners Attitudes and Opinions," in *2013 Information Security for South Africa*, Johannesburg, South Africa, 2013.

[53] M. Gül and E. Kugu , "A Survey on Anti-Forensics Techniques," in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)* , Malatya, Turkey , 2017.

[54] C. Janssen, "Steganography," 2014.

[55] S. Rekhis and N. Boudriga, "Formal Digital Investigation of Anti-Forensic Attacks," in *2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, Oakland, CA, USA, 2010.

[56] M. Chernyshev, S. Zeadally, Z. Baig and A. Woodward, "Mobile Forensics: Advances, Challenges, and Research Opportunities," *IEEE Security & Privacy,* vol. 15, no. 6, pp. 42-51, 2017.

[57] D. Lillis, B. A. Becker, T. O'Sullivan and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in *Annual ADFSL Conference on Digital Forensics, Security and Law*, Florida, USA, 2016.

[58] X. Du, N.-A. Le-Khac and M. Scanlon, "Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service," in *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS 2017)*, Dublin, Ireland, 2017.

[59] A. Roder, K. Choo and N. Le-Khac, "Unmanned Aerial Vehicle Forensic Investigation Process: DJI Phantom 3 Drone As a Case Study," in *13th Annual ADFSL Conference on Digital Forensics, Security and Law*, San Antonio, 2018.

[60] S. Alabdulsalam, K. Schaefer, T. Kechadi and N.-A. LeKhac, "Internet of things forensics: Challenges and case study," in *Advances in Digital Forensics XIV: 14th Annual IFIP WG11.9 International Conference on Digital Forensics*, New Delhi, India, 2018.

[61] A. MacDermott, T. Baker and Q. Shi, "IoT Forensics: Challenges for the IoA Era," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Paris, France, 2018.

[62] Council of Europe, Budapest Convention on Cybercrime, 2001.

[63] *Edmund Addo v the Republic of Ghana,* 2017.

[64] G. Kessler, "Judges' Awareness, Understanding and Application of Digital Evidence," *Journal of Digital Forensics, Security and Law,* vol. 6, no. 1, Article 4, 2011.

[65] C. Brown, Computer Evidence: Collection and Preservation, Boston, MA: Course Technology, 2010.

[66] S. Mason, International Electronic Evidence, British Institute of International and Comparative Law, 2008.

[67] O. S. Kerr, Computer Crime Law, 2nd ed., St. Paul. MN:Thomson/West, 2009.

[68] B. Garner, Black's Law Dictionary, St. Paul, Minnesota: West Publishing, 1999.

[69] S. Brobbey, Essentials of the Ghana Law of Evidence, Accra, Ghana: Datro Publications, 2014.

[70] P. Stephenson, Investigating Computer-Related Crime, Boca Raton, Florida: CRC Press, 2000.

[71] *Daubert v Merrell Dow Pharmaceuticals, Inc, 509 U.S. 579,* 1993.

[72] T. J. Cowper and B. H. Levin, "Autonomous Vehicles: How Will They Challenge Law Enforcement?," 13 February 2018. [Online]. Available: https://leb.fbi.gov/articles/featured-articles/autonomous-vehicles-how-will-they-challenge-law-enforcement. [Accessed 12 January 2019].

[73] R. Saferstein, Criminalistics: An Introduction to Forensic Science, Pearson, 2000.

[74] P. Sommer, "Digital footprints: Accessing Computer Evidence," *Criminal Law Review,* pp. 61-78, 2000.

[75] R. Mercuri, "Challenges in Forensic Computing.," *Communications of the ACM 48,* pp. 17 - 21, 2005.

[76] S. Janes, "The Role of Technology in Computer Forensic Investigations," *Information Security Technical Report,* vol. 5, pp. 43 - 50, 2000.

[77] K. J. Flusche, "Computer Forensic Case Study: Espionage, Part 1 Just Finding the File is not Enough!," *Information Security Journal,* vol. 10, pp. 1 - 10, 2001.

[78] M. A. Caloyannides, Computer Forensics and Privacy, Norwood, Minnesota: Artech House, 2001.

[79] P. Akester, "Internet Law: Authenticity of Works: Authorship and Authenticity in Cyberspace," *Computer Law & Security Report,* pp. 436-444, 2004.

[80] E. E. Kenneally, "Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection," *UCLA Journal of Law and Technology,* 2005.

[81] L. Strydom, "Computer Evidence," in *2nd World Conference on the Investigation of Crime*, ICC Durban, 2001.

[82] S. Mason, Electronic Evidence, 3 ed., London, United Kingdom: Butterworths Law, 2012.

[83] U.S Committee on the Judiciary, Federal Rules of Evidence, Rule 702. Testimony by Expert Witnesses, Washington: U.S. Government Printing Office, 2014.

[84] D. J. Ryan and G. Shpantzer, "Legal Aspects of Digital Forensics," [Online]. Available: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf.

[85] E. Roffeh, Practical Digital Evidence - Part I: Law and Technology, 2014.

[86] O. Leroux, "Legal Admissibility of Electronic Evidence," *International Review of Law, Computers and Technology,* vol. 18, no. 2, pp. 193-220, 2004.

[87] J. T. Ami-Narh and P. Williams, "Digital Forensics and the Legal System: A Dilemma of Our Times," in *Proceedings of the 6th Australian Digital Forensics Conference*, 2008.

[88] U.S Committee on the Judiciary, Federal Rules of Evidence, Rule 102. Purpose, Washington: U.S. Government Printing Office, 2014.

[89] M. Meyers and M. Rogers, "Computer Forensics: The Need for Standardization and Certification," *International Journal of Digital Evidence,* vol. 3, no. 2, 2004.

[90] E. Kalaimannan , "Smart Device Forensics - Acquisition, Analysis and Interpretation of Digital Evidences," in *2015 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2015.

[91] International Organization for Standardization, Information Technology - Security Techniques - Guidance on Assuring Sustainability and Accuracy of Incident Investigative Methods, ISO/IEC 27041:2015 Standard, Geneva, Switzerland, 2015.

[92] National Forensic Science Technology Centre, Crime Scene Investigation: A Guide for Law Enforcement, Largo, Florida, 2013.

[93] G.Giova, "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems," *International Journal of Computer Science and Network Security,* vol. 11, no. 1, 2011.

[94] C. Vecchio-Flaim, Developing a Computer Forensics Team, Bethesda, Maryland: SANS Institute, InfoSec Reading Room, 2001.

[95] Office of Law Enforcement Standards, National Institute of Standards and Technology and the National Institute of Justice, "Association of Crime Laboratory Directors; Forensic Laboratories: Handbook for Facility Planning, Design, Construction, and Moving," U. S. Department of Justice, Washington, 1998.

[96] H. Henseler and . S. v. Loenhout , "Educating Judges, Prosecutors and Lawyers in the use of Digital Forensic Experts," in *Proceedings of the Fifth Annual DFRWS Europe*, Florence, Italy, 2018.

[97] S. Schroeder, "How to be a Digital Forensic Expert Witness," in *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, Taipei, Taiwan, Taiwan, 2005.

[98] K. Murff, H. Gardenier and M. Gardenier, "Digital Forensics and the Law," in *Conference on Digital Forensics, Security and Law*, Richmond, Virginia , 2011.

[99] D. Garrie and J. Morrissy, "Digital Forensics Evidence in the Courtroom: Understanding Content and Quality," *North Western Journal of Technology and Intellectual Property,* vol. 12, no. 2, Article 5, 2014.

[100] *The Republic of Ghana v Alexander Kofi Tweneboah, Suit No. TB 15/13/15, Financial Crimes Court,* 2016.

[101] Z. Zhao, "A Framework to Analyze Reliability of Digital Evidences in Computer Systems," in *2015Sixth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA)*, Guiyang, China, 2015.

[102] É. O'Brien, . N. N. Daeid and S. Black, "Science in the Court: Pitfalls, Challenges and Solutions," *Philosophical Transactions of the Royal Society B: Biological Sciences. https://doi.org/10.1098/rstb.2015.0062,* vol. 370, no. 1674, 2015.

[103] T. Poole, "Proportionality in Perspective," in *LSE Law, Society and Economy Working Papers 16/2010* , 2010.

[104] R. Trotter, "Qualitative Research Sample Design and Sample Size: Resolving and Unresolved Issues and Inferential Imperatives," *Preventive Medicine Journal ,* no. 55, p. 398–400, 2012.

[105] D. Bertram, "Likert Scales: Are the Meaning of Life," 2008. [Online]. Available: http://poincare.matf.bg.ac.rs/~kristina/topic-dane-likert.pdf. [Accessed 27 April 2018].

[106] I. Etikan and K. Bala, "Sampling and Sampling Methods," *Biometrics and Biostatistics International Journal,* vol. 5, no. 6, 2017.

[107] S. Weller and A. Romney, Systematic Data Collection, Qualitative Research Methods, vol. 10, Sage Publications., 1988.

[108] D. Child, The essentials of Factor Analysis, 3rd ed., New York: Continuum International Publishing Group, 2006.

[109] H. Taherdoost , "Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research," *International Journal of Academic Research in Management (IJARM) ,* vol. 5, no. 3, pp. 28-36, 2016.

[110] L. J. Burton and S. M. Mazerolle, "Survey Instrument Validity Part I: Principles of Survey Instrument Development and Validation in Athletic Training Education Research," *Athletic Training Education Journal,* vol. 6, no. 1, pp. 27-35, 2011.

[111] "Statistics How To: Statistics for the Rest of Us, Practically Cheating Statistics Handbook, Kaiser-Meyer-Olkin (KMO) Test for Sampling Adequacy," 2016. [Online]. Available: http://www.statisticshowto.com/kaiser-meyer-olkin/.

[112] Organisation for Economic Co-operation and Development, Handbook on Constructing Composite Indicators: Methodology and User Guide, Paris: OECD Publishing, 2008.

[113] A. Bryman and D. Cramer, Constructing Variables, Handbook of Data Analysis, M. Hardy and A. Bryman , Eds., SAGE Publications, 2004.

[114] A. Field, Discovering Statistics Using SPSS: Introducing Statistical Method, 3rd, Ed., Thousand Oaks, Califonia: Sage Publications, 2009.

[115] Statistics Solutions , "Univariate and Multivariate Outliers," [Online]. Available: http://www.statisticssolutions.com/univariate-and-multivariate-outliers/. [Accessed 27 September 2018].

[116] R. Gorsuch, Factor Analysis, 2nd, Ed., Hillside, NJ: Lawrence Erlbaum Associates, 1983.

[117] Study.com, "Pearson Correlation Coefficient: Formula, Example & Significance," 2016. [Online]. Available: https://study.com/academy/lesson/pearson-correlation-coefficient-formula-example-significance.html.

[118] StataCorp, "Stata Statistical Software," StataCorp LLC, [Online]. Available: https://www.stata.com/why-use-stata/.

[119] D. D. Brewer, "Regression and correlation," 2001. [Online]. Available: http://faculty.washington.edu/ddbrewer/s231/s231regr.htm. [Accessed 27 September 2018].

[120] H. Kaiser, "The Application of Electronic Computers to Factor Analysis," *Educational and Psychological Measurement,* vol. 20, no. 1, pp. 141-151, 1960.

[121] A. G. Yong and S. Pearce, , "A Beginner’s Guide to Factor Analysis: Focusing on Exploratory Factor Analysis," *Tutorials in Quantitative Methods for Psychology,* vol. 9, no. 2, pp. 79-94, 2013.

[122] "Ghana: Act No. 29 of 1960, Criminal Offences Act," 1960. [Online]. Available: http://laws.ghanalegal.com/acts/id/19.

[123] D. Wang and K. Wang , "The Implementation of Tempering Justice with Mercy Criminal," in *2nd International Conference on Social Science and Humanity, IPEDR*, Singapore, 2012.

APPENDIX A: ACRONYMS USED

The purpose of this appendix is to introduce the various acronyms used in the thesis and their corresponding meanings. Some of the acronyms already exist in literature whilst others were introduced into the thesis.

ACPO	The Association of Chief Police Officers
ASCLD	American Society of Crime Laboratory Directors
CFA	Confirmatory Factor Analysis
CFRF	Cloud Forensic Readiness Framework
CoC	Chain of Custody
CoE	Council of Europe
DAT	Determinant Assessment Toolkit
DEA	Digital Evidence Authenticity
DEI	Digital Evidence Integrity
DEP	Digital Evidence Proportionality
DERe	Digital Evidence Relevance
DERl	Digital Evidence Reliability
DFEW	Digital Forensics Expert Witness
DFL	Digital Forensics Lab
DFM	Digital Forensics Model
DFR	Digital Forensics Report
DFRWS	Digital Forensics Research Workshop
DOJ	Department of Justice
EFA	Exploratory Factor Analysis
EW	Evidential Weight

FA	Factor Analysis
FAC	Forensic Analyst Competency
FT	Forensic Tools
HM-DEAA	Harmonised Model for Digital Evidence Admissibility Assessment
HM-DEAA ExP	HM-DEAA Expert System
IoT	Internet of Things
ISO	International Organization for Standardization
KMO	Kaiser-Meyer- Olkin
LA	Legal Authorisation
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
PPA	Privacy Protection Act
SOPs	Standard Operating Procedures
SWGDE	Scientific Working Group on Digital Evidence
TIV	Technical Integrity Verification
UAVs	Unmanned Aerial Vehicles

APPENDIX B: DEFINITION OF TERMINOLOGIES

This appendix provides detailed explanation of the various terminologies that were introduced in the thesis. The purpose of this is to ensure clarity and address any potential ambiguity associated with the term as used within the context of the thesis.

Anti-Forensic A general term which refers to a set of techniques used as countermeasures to forensic analysis.

Centre of Gravity This is a terminology which has been introduced into this research. The term is used to denote the increasing use of the cyberspace for criminal activities. The fact underlying the introduction of this terminology is the current transformation of crimes of which the cyber space has become its foundation.

Criminology The scientific study of crime and criminals.

Crypto-technologies A system that provides a distributed recording system, which guarantees the possibility of identifying irrefutable transactional data.

Cyber-Dependent Crimes Cyber-dependent crimes generally refer to network-centric crimes. They can only be committed using a computer, networks or any other information technology infrastructure or digital device. Examples of such crimes include hacking and denial of service (DoS) attacks.

Cyber-Facilitated Crimes Cyber-facilitated crimes are conventional crimes, which are perpetrated using computers, network technologies or any other information technology infrastructure or digital device. Examples of such cases include, human trafficking, terrorism and economic crimes such as financial fraud and money laundering.

Cyberspace

The virtual computer world, and more specifically, an electronic medium used to form a global computer network to facilitate online communication.

Dark net

The darknet refers to networks that are not indexed by search engines and is only accessible via authorisation, specific software and configurations.

Dark web

A part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or and to a certain degree, untraceable.

Determinant

The word ‘determinant’ is used in the thesis to refer to the requirements, benchmarks, and/or factors that are considered during judicial proceedings in admitting a particular digital evidence.

Determinant Assessment Toolkits

This terminology is introduced into this research to reference a set of tools in the form of assessment questions and considerations, which provide guidance to judicial authorities in scoring each determinant when assessing digital evidence admissibility.

Determinant Weight This terminology is introduced in this research to explain the weight of each determinant as established through the Factor Analysis (FA).

Determinant Score This terminology is introduced in this research to represent the score assigned to each of the determinants by a judge or a court in a case under judicial consideration.

Digital Evidence According to ISO/IEC 27037, digital evidence is information or data, stored or transmitted in binary form, that may be relied upon as evidence. Digital evidence is a typology of evidence, derived from digital forensics processes, procedures and activities.

Digital Evidence Interoperability This is a terminology which has been introduced into this research. The term refers to the increasing requirements for legal harmonisation for the purposes of digital evidence exchange across different jurisdictions for the purposes of investigating and prosecuting trans-border cybercrime.

Digital Forensics The application of science to the identification, collection, examination, and analysis, of data whilst preserving the integrity of the information and maintaining a strict chain of custody for the data.

Digital Footprints This terminology generally refers to a trail of data that one creates whilst using the Internet. Internet users normally leave their digital footprints online.

Encryption Technology This refers to a computing technology that is designed to encode a message or information in such a way that only authorised parties can access it. Encryption technology normally helps to convert plaintext into cyphertext.

Evidence Black's Law Dictionary defines evidence as 'any species of proof, or probative matter, legally presented at the trial of an issue, by the act of parties and through the medium of witnesses, records, documents, exhibits, concrete objects, etc. for the purpose of inducing belief in the minds of the court or jury as their contention.'

Exhibit An exhibit, in legal proceedings, is physical or documentary evidence brought before a judge or a jury during a trial.

Evidential Weight Evidential weight is a weight that a judge will usually attach to any evidence that is tendered in court during a trial. In the application of the HM-DEAA model, evidential weight is given by the summation of the Weighted Values (Wv).

Factor Analysis Factor analysis is a known statistical method used to describe variability among observed, correlated variables in terms of a potentially lower number of unobserved variables, usually called factors. The two main factor analysis techniques are Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA). Factor analysis has been adopted in this research to construct the weights of the various variables required for making judicial decisions.

Forensic-by-Design Forensic-by-Design is a concept that relates to the integration of forensic requirements into the design, development and implementation of a computing architecture or an IT system for the purpose of enhancing forensic readiness of the target architecture, system or environment.

Forensic Examiner A professional who conducts forensic examinations in any of the forensic science fields.

Harmonised Model for Digital Evidence Admissibility Assessment This is a model that has been introduced in this research to assess digital evidence admissibility and to determine the evidential weight of digital evidence in judicial proceedings.

Hash Algorithms A mathematical function that converts a piece or a set of digital data into a constant numeral representation, usually used in digital forensics to ensure the integrity of digital evidence. Message-Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA-1) are the two common hash algorithms that are employed in digital forensics mainly for the purposes of evidence integrity.

HM-DEAA ExP The HM-DEAA ExP is a software expert system that has been developed to automate the operations of the HM-DEAA model.

Internet of Things Internet of Things (IoT) refers to the connectivity of mainly physical devices and objects such as vehicles, home appliances devices and electronics, and the networks that allow these devices to interact, collect store, and exchange data.

Sakawa This refers to a particular trend of cybercrime activities involving perpetrators in Ghana. The term has a techno-spiritual connotation because the practice combines internet-based illegal activities with fetish rituals.

Scientificity This terminology refers to the quality or the state of being scientific. Scientific methods are processes and procedures that are based on the principles of science.

Technical Determinants This terminology has been introduced into this research to describe a number of technical requirements comprising of both activities, approaches, standards, procedures and processes that underpin the scientific method through which digital evidence is produced. Judicial considerations pertaining to the admissibility of digital evidence and determination of evidential weight of digital evidence are fundamentally based on these determinants.

Techno-Legal Dilemma This is a concept that has been introduced into the research to define the research's core problem statement. This concept refers to the difficulty or the existing gap of establishing a balanced but also an interdependent relationship between the various technical and the legal determinants for the purposes of establishing a harmonised scientific foundation to aid the admissibility of digital evidence in judicial proceedings.

The Onion Router (TOR) An open-source software that allows for anonymous communication over the internet. Users normally deploy TOR-based internet technologies to protect their privacy and security against internet-based surveillance. Increasingly, TOR-based technologies are being used for criminal activities.

Weighted Value It represents the evidential weight of a specific determinant. In the application of the HM-DEAA model, Weighted Value is given by the product of the Determinant Weight and the Determinant Score.

Write Blockers Write blockers are devices or applications that allow acquisition of information from a digital storage media without creating the possibility of tampering (intentional or accidental) the contents of the target digital media.

APPENDIX C: SURVEY QUESTIONNAIRE — ADMISSIBILITY OF DIGITAL EVIDENCE

This appendix provides a template of the questionnaire that was administered to survey participants as explained in Chapter 6. The questionnaire was administered in order to validate the model adopted for this study. As part of the questionnaire, respondents' consent was sought before proceeding to the actual survey. The questionnaire was administered online using SurveyGizmo; a platform for building online forms and surveys for research projects.

CONSENT

Respondent hereby voluntarily grant permission for participation in the survey project as explained above. The objectives of the survey project are clear to me and I understand my right to choose whether to participate in the survey project or not. I understand that the information furnished will be handled confidentially and that the results of the survey may be used for the purposes of publication.

I give my consent to proceed with the survey □

A. BACKGROUND OF SURVEY RESPONDENT

SN	Item	Response
1	Job Title	
2	Summary of Job Role	
3	Brief Experience with Digital Evidence	
4	Geographical Region/Country	

B. RESEARCH QUESTIONS:

1. Which of the following technical factors/determinants affect the admissibility of digital evidence? How do you rate the impact of each of the determinants on evidential weight of a piece of digital evidence, using the scale of 1–5? *1 = No Impact, 2 = Minimal Impact, 3 = Moderate Impact, 4 = Significant Impact, 5 = Very Significant Impact*

SN	Technical Determinant	Determinant Description *(Summary)*	Affect Evidence Admissibility? *(YES or NO)*	Impact on Evidential Weight *(Using a scale of 1–5)*
1	Digital Forensics Model Determinant	Adopting an appropriate digital forensics approach or procedure for collection, processing and presentation of digital evidence.		
2	Forensic Tools Determinant	Using an appropriate digital forensics tool (software or hardware) for collection, processing and presentation of digital evidence.		
3	Chain of Custody Determinant	Processes, procedures and activities involved in the preservation of the integrity of digital evidence (audit trails).		
4	Forensic Analyst Competency Determinant	Qualification and experience of an Analyst or a Forensic Examiner in the collection, processing and presentation of digital evidence.		
5	Digital Forensics Lab Determinant	Availability of a forensic lab for the collection, processing and presentation of digital evidence (for digital forensic quality assurance).		
6	Technical Integrity Verification Determinant	The use of technical controls and measures (such as use of Write Blockers, Hash Values, etc.) to prevent copying or modification of digital evidence.		
7	Digital Forensics Expert Witness Determinant	The opinion of technical expert witness (if required) in a case (before a court) involving digital evidence.		
8	Digital Forensics Report Determinant	The manner in which digital evidence and investigation findings are presented (in a form of a report) to the court.		

2. Are there any other technical determinants which impact on the admissibility of digital evidence which is not listed above? Kindly list any and indicate its impact on evidential weight, using the scale of 1–5? *1 = No Impact, 2 = Minimal Impact, 3 = Moderate Impact, 4 = Significant Impact, 5 = Very Significant Impact*

SN	**Technical Determinant** *(To be filled by survey respondents)*	**Determinant Description** *(Summary)*	**Affect Evidence Admissibility** *(YES or NO)*	**Impact on Evidential Weight** *(Using a scale of 1–5)*
1				
2				
3				
4				

3. Which of the following legal determinants affect the admissibility of digital evidence? How do you rate the impact of each of the determinants on evidential weight of a piece of digital evidence, using the scale of *1–5*? *1 = No Impact, 2 = Minimal Impact, 3 = Moderate Impact, 4 = Significant Impact, 5 = Very Significant Impact*

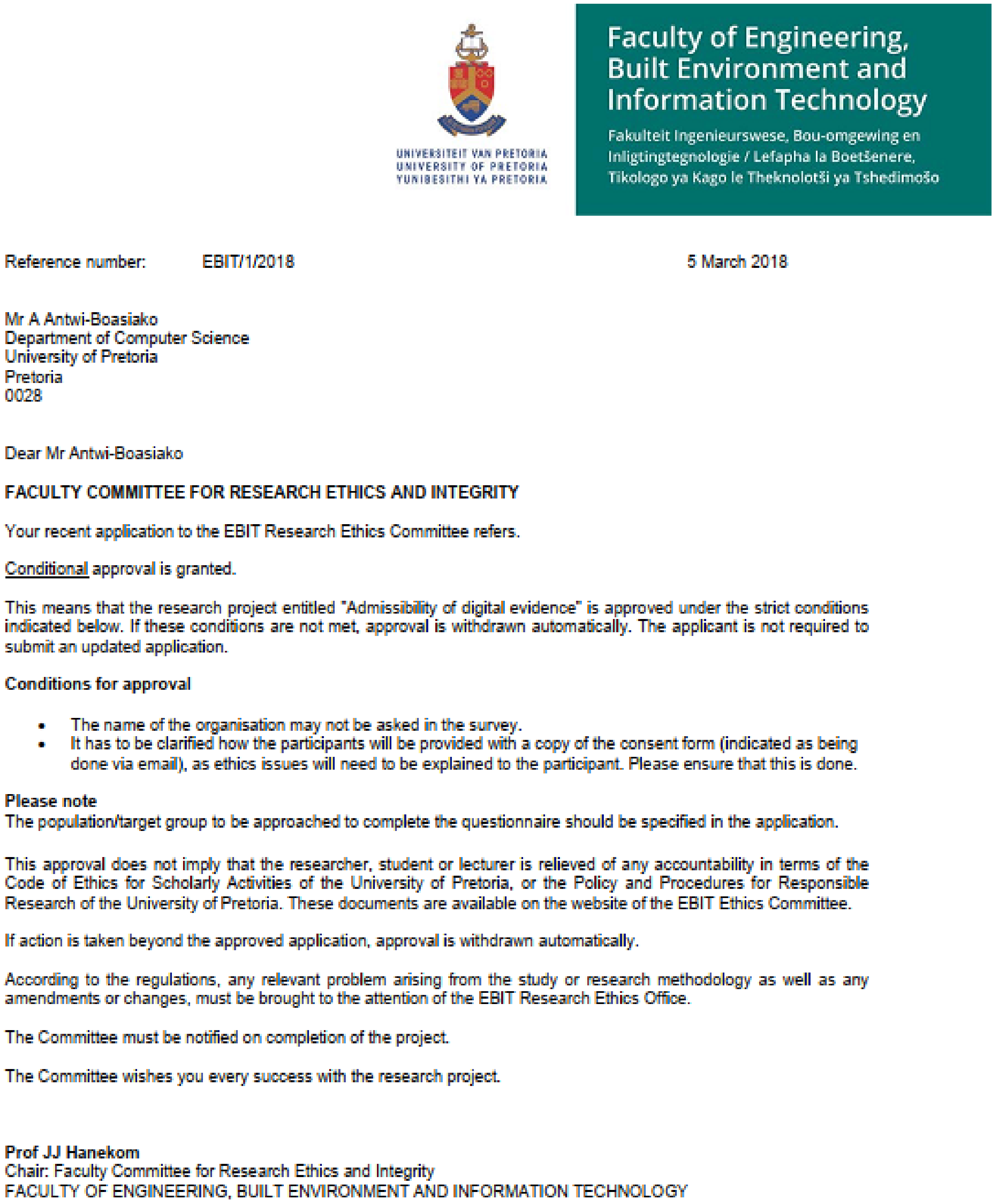
SN	Legal Determinant	Determinant Description *(Summary)*	Affect Evidence Admissibility? *(YES or NO)*	Impact on Evidential Weight *(Using a scale of 1–5)*
1	Legal Authorisation Determinant	Legal determinant or basis for searching, seizing and analysing devices or computer systems for digital evidence.		
2	Digital Evidence Relevance Determinant	The determinant requires that a digital evidence under consideration should be capable of proving or disproving a case before a court.		
3	Digital Evidence Authenticity Determinant	The determinant requires that the evidence must establish facts in a way that cannot be disputed and is a true representation of the original.		
4	Digital Evidence Integrity Determinant	The determinant requires that digital evidence should be complete and unaltered.		
5	Digital Evidence Reliability Determinant	The determinant requires that no aspect of digital evidence being introduced at a trial should be doubtful.		
6	Digital Evidence Proportionality Determinant	The determinant that obliges a digital forensics investigator to obtain only information or electronic data that the law has authorised to be accessed.		

4. Are there any other legal determinants which impact on the admissibility of digital evidence which is not listed above? Kindly list any and indicate its impact on evidential weight, using the scale of 1–5? *1 = No Impact, 2 = Minimal Impact, 3 = Moderate Impact, 4 = Significant Impact, 5 = Very Significant Impact*

SN	Legal Determinant *(To be filled by survey respondents)*	Determinant Description *(Summary)*	Affect Evidence Admissibility? *(YES or NO)*	Impact on Evidential Weight *(Using a scale of 1–5)*
1				
2				
3				
4				

APPENDIX D: ETHICAL CLEARANCE

This appendix shows the ethical clearance that the researcher obtained from the University of Pretoria, as mentioned in Chapter 6. This was a requirement from the University before the survey questionnaire; shown in Appendix C was administered.



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Engineering, Built Environment and Information Technology

Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie / Lefapha la Boetšenere, Tikologo ya Kago le Theknolotši ya Tshedimošo

Reference number: EBIT/1/2018 5 March 2018

Mr A Antwi-Boasiako
Department of Computer Science
University of Pretoria
Pretoria
0028

Dear Mr Antwi-Boasiako

FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Research Ethics Committee refers.

Conditional approval is granted.

This means that the research project entitled "Admissibility of digital evidence" is approved under the strict conditions indicated below. If these conditions are not met, approval is withdrawn automatically. The applicant is not required to submit an updated application.

Conditions for approval

- The name of the organisation may not be asked in the survey.
- It has to be clarified how the participants will be provided with a copy of the consent form (indicated as being done via email), as ethics issues will need to be explained to the participant. Please ensure that this is done.

Please note
The population/target group to be approached to complete the questionnaire should be specified in the application.

This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Code of Ethics for Scholarly Activities of the University of Pretoria, or the Policy and Procedures for Responsible Research of the University of Pretoria. These documents are available on the website of the EBIT Ethics Committee.

If action is taken beyond the approved application, approval is withdrawn automatically.

According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of the EBIT Research Ethics Office.

The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.

Prof JJ Hanekom
Chair: Faculty Committee for Research Ethics and Integrity
FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

Figure D.1: Ethical Clearance

APPENDIX E: SURVEY RESPONDENT'S GEOGRAPHICAL AND LEGAL JURISDICTIONS

This appendix shows a distribution of the number of respondents that participated in the survey and their geographical and legal jurisdictions. Respondents were drawn from Africa, North and South America, Asia, Europe and Middle East. This is further discussed in Chapter 6.

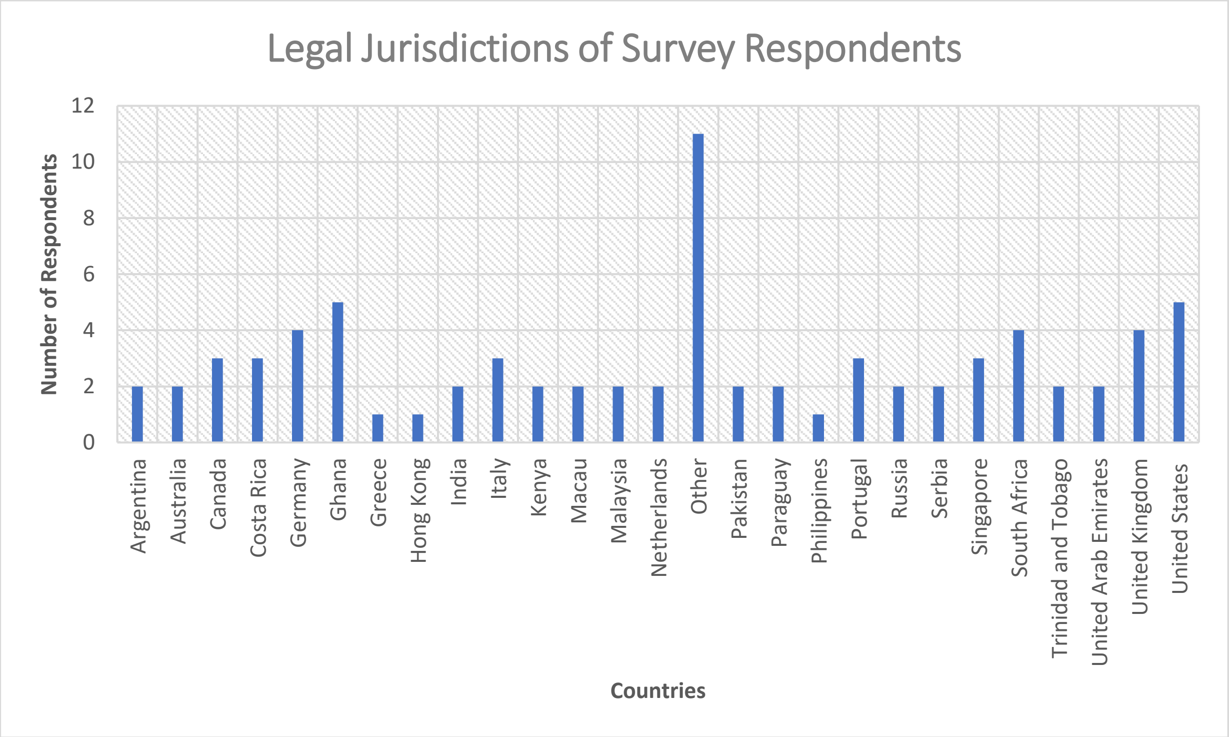


Figure E.1: Graph showing Respondent's Geographical and Legal Jurisdictions

APPENDIX F: DETERMINANT ASSESSMENT QUESTIONS

This appendix provides a list of assessment questions that were used to allocate scores for the various determinants. These assessment questions were introduced into the thesis as part of the survey and the case study involving the ten (10) judicial cases discussed in Chapter 9. The list of the assessment questions for each determinant is however, not exhaustive. Chapter 8 also explains the use of the assessment questions in the implementation of the HM-DEAA Expert System.

Table F.1: Technical Determinant Assessment Questions

Technical Determinant	**Assessment Questions**
Digital Forensics Model Determinant	• What digital forensic approach did you adopt for the investigations and what is the justification? • Is the model adopted suitable for the forensic examination? • Does the model conform to the digital forensics processes and procedure guidelines? • How scientific is the model used for the forensic examination? • Any specific scientific publications on the model?
Forensics Tools Determinant	• Which tool was used for forensic examination? • Was the digital forensics tool used licensed? • Has the tool been tested/validated? By which body/institution? • Has the tool been previously used in a similar case in another court, either in Ghana or in a similar legal jurisdiction? • Is the tool open-source or proprietary? Are they any impact of the tool on the digital evidence processed? • Does the tool have any recorded error rate? • What is the level of acceptance of the tool among digital forensic examiners and researchers? • Any scientific publication(s) on the tool?
Chain of Custody Determinant	• Is there a paper trail in connection with the collection, storage and the general handling of the exhibit involved in the case? • Are the exhibits properly and accurately labelled? • Any broken chain of custody • Is the chain-of-custody complete and accurate?
Digital Forensic Lab Determinant	• Dedicated computer for analysis • Forensics computer with licensed Operating System • Evidence collection accessories • Evidence preservation devices • Secured evidence storage • Access control • Does forensic lab have SOP?
Forensic Analyst Competency Determinant	• Level of education • Is the Analyst certified? • Years of experience • Previous experience in handling a similar case
Technical Integrity Verification Determinant	• Was write blockers used • Are there hash values of the evidence available? • Was storage device wipe prior to storing evidence? • Was forensic image created?

Technical Determinant	**Assessment Questions**
Digital Forensics Expert Witness Requirement and Assessment	• Is the expert witness certified? • Years of experience • Scientific/Technical Knowledge • Ever testified in court?
Digital Forensic Report Determinant	• Is the forensic methodology adopted well documented in the report? • Is the evidence labelling accurate and complete in the report? • Is the case file documentation complete and detailed such that another examiner can recreate the results of the examination(s)? • Does the report indicate the tools used for the forensic examination? • Were the examination results peer reviewed?

Table F.2: Legal Determinant Assessment Questions

Legal Determinant	Assessment Questions
Legal Authorisation Determinant	• Was legal authorisation obtained before the digital device was seized? • What kind of legal authorisation did you obtain? • What was the scope of the legal authorisation obtained? • Was the expert authorised to examine the exhibit?
Digital Evidence Relevance Determinant	• Is the evidence user or system generated? • Is the evidence relevant to the case? • What is the source of the evidence? • How credible is the source? • Can evidence prove or disprove the case?
Digital Evidence Authenticity Determinant	• Is the evidence user generated? • Does the evidence link to the accused? • Was the evidence extracted from the device under examination?
Digital Evidence Integrity Determinant	• Was write blockers used • Are there hash values of the evidence available? • Was storage device wiped prior to storing evidence? • Is the chain-of-custody complete and accurate? • Was the evidence securely stored?
Digital Evidence Reliability Determinant	• Were the techniques used in collecting the evidence tested? • Did the techniques undergo peer review? • What is the error rate associated with the technique? • Is the technique accepted by the scientific community? • Is the technique adopted in the forensic examination based on any standard?
Digital Evidence Proportionality Determinant	• What is the scope of your investigations? • What safeguards did you put in place to ensure the privacy of the suspect? • What search terms did you use in analysing the contents of the digital device? • Are the search terms consistent with the legal authorisation obtained for the seizure? • Is the evidence obtained within the scope of the search warrant?

APPENDIX G: CORRELATION BETWEEN DETERMINANTS

The table in this appendix shows a detailed result from the Pearson Correlation analysis that the dataset was subjected to. The analysis shows that, there is a correlation that exist between the various determinants. The procedure for calculating the correlation is also provided in this section. The procedure presented below was used to calculate the correlation coefficient of the data in the dataset. The example below focuses on calculating the correlation coefficient between the Digital Forensics Model (DFM) and Forensics Tools (FT) determinants using the Pearson Correlation Coefficient formula. The formula is given by;

$$r = \frac{N\sum xy - (\sum x)(\sum y)}{\sqrt{[N\sum x^2 - (\sum x)^2][N\sum y^2 - (\sum y)^2]}}$$

Where

x represents the values of response for DFM determinant

y represents the values of response for FT determinant

N = number of respondents

The sum of all x values from the dataset, $\Sigma\,x = 92416$

The sum of all y values from the dataset, $\Sigma\,y = 92416$

Summation of xy values from the dataset, $\Sigma\,xy = 1263$

Summation of x^2 values from the dataset, $\Sigma\,x^2 = 1324$

Summation of y^2 values from the dataset, $\Sigma\,y^2 = 1330$

N = 75

Substituting the variables in the Pearson Correlation Coefficient formula;

$$r = \frac{75 * 1263 - (304)(304)}{\sqrt{[75 * 1324 - (304)^2][75(1330) - (304)^2]}}$$

$$r = \frac{94725 - 92416}{\sqrt{[99300 - 92416][99750 - 92416]}}$$

$$r = \frac{2309}{\sqrt{[6884][7334]}}$$

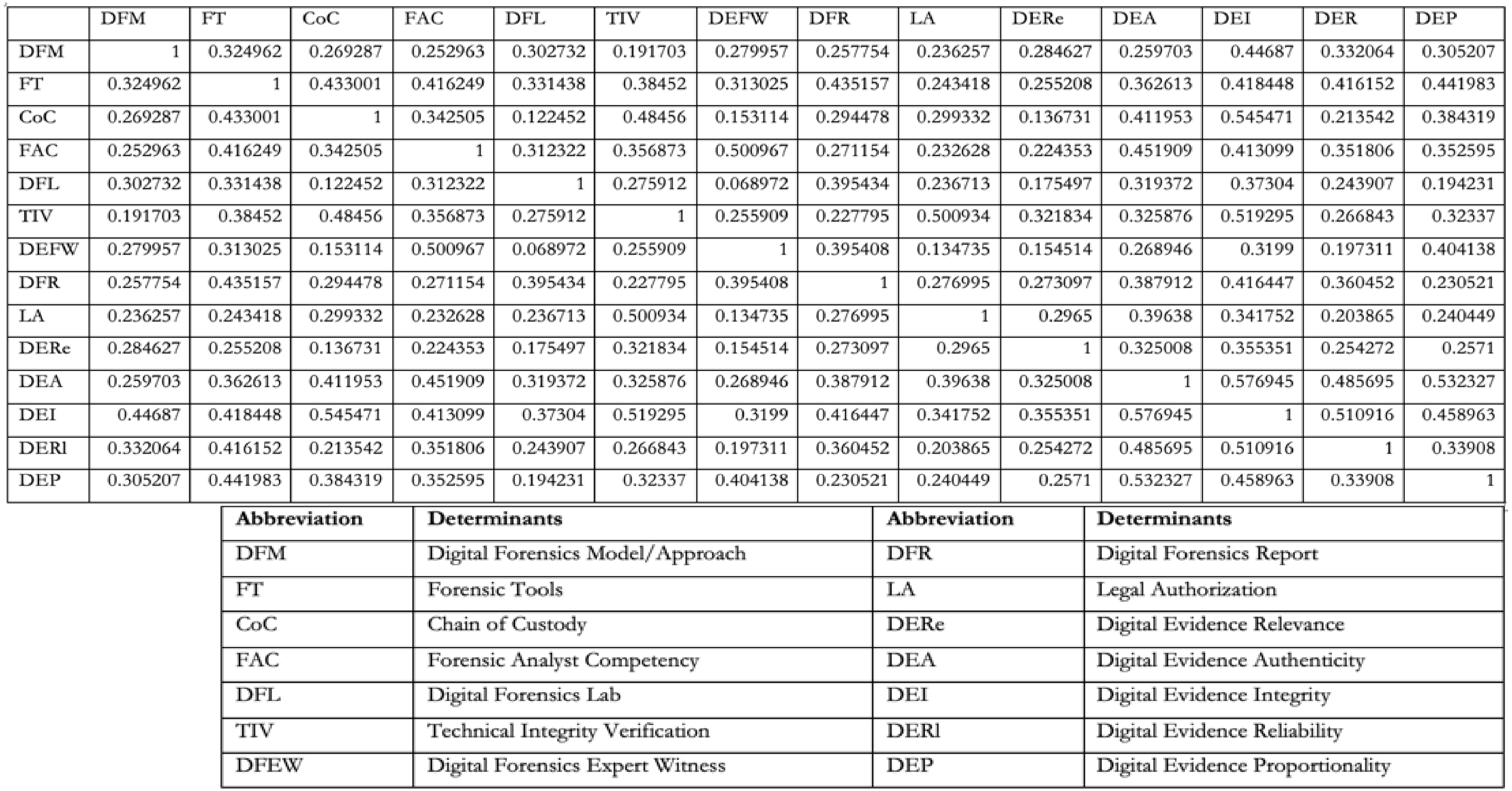
$$r = \frac{2309}{\sqrt{[50487256]}}$$

$$r = \frac{2309}{7105.43848}$$

$$r = 0.324962$$

Therefore, the correlation coefficient value for DFM and FT is 0.324962. This value implies the relationship between DFM and FT is mild since the value lies between the 0.2 to 0.4 as explained in Chapter 7. The same procedures were applied to determine the correlation between rest of the determinants shown in Table G.1

Table G.1: Correlation between Determinants



	DFM	FT	CoC	FAC	DFL	TIV	DEFW	DFR	LA	DERe	DEA	DEI	DER	DEP
DFM	1	0.324962	0.269287	0.252963	0.302732	0.191703	0.279957	0.257754	0.236257	0.284627	0.259703	0.44687	0.332064	0.305207
FT	0.324962	1	0.433001	0.416249	0.331438	0.38452	0.313025	0.435157	0.243418	0.255208	0.362613	0.418448	0.416152	0.441983
CoC	0.269287	0.433001	1	0.342505	0.122452	0.48456	0.153114	0.294478	0.299332	0.136731	0.411953	0.545471	0.213542	0.384319
FAC	0.252963	0.416249	0.342505	1	0.312322	0.356873	0.500967	0.271154	0.232628	0.224353	0.451909	0.413099	0.351806	0.352595
DFL	0.302732	0.331438	0.122452	0.312322	1	0.275912	0.068972	0.395434	0.236713	0.175497	0.319372	0.37304	0.243907	0.194231
TIV	0.191703	0.38452	0.48456	0.356873	0.275912	1	0.255909	0.227795	0.500934	0.321834	0.325876	0.519295	0.266843	0.32337
DEFW	0.279957	0.313025	0.153114	0.500967	0.068972	0.255909	1	0.395408	0.134735	0.154514	0.268946	0.3199	0.197311	0.404138
DFR	0.257754	0.435157	0.294478	0.271154	0.395434	0.227795	0.395408	1	0.276995	0.273097	0.387912	0.416447	0.360452	0.230521
LA	0.236257	0.243418	0.299332	0.232628	0.236713	0.500934	0.134735	0.276995	1	0.2965	0.39638	0.341752	0.203865	0.240449
DERe	0.284627	0.255208	0.136731	0.224353	0.175497	0.321834	0.154514	0.273097	0.2965	1	0.325008	0.355351	0.254272	0.2571
DEA	0.259703	0.362613	0.411953	0.451909	0.319372	0.325876	0.268946	0.387912	0.39638	0.325008	1	0.576945	0.485695	0.532327
DEI	0.44687	0.418448	0.545471	0.413099	0.37304	0.519295	0.3199	0.416447	0.341752	0.355351	0.576945	1	0.510916	0.458963
DERl	0.332064	0.416152	0.213542	0.351806	0.243907	0.266843	0.197311	0.360452	0.203865	0.254272	0.485695	0.510916	1	0.33908
DEP	0.305207	0.441983	0.384319	0.352595	0.194231	0.32337	0.404138	0.230521	0.240449	0.2571	0.532327	0.458963	0.33908	1

Abbreviation	Determinants	Abbreviation	Determinants
DFM	Digital Forensics Model/Approach	DFR	Digital Forensics Report
FT	Forensic Tools	LA	Legal Authorization
CoC	Chain of Custody	DERe	Digital Evidence Relevance
FAC	Forensic Analyst Competency	DEA	Digital Evidence Authenticity
DFL	Digital Forensics Lab	DEI	Digital Evidence Integrity
TIV	Technical Integrity Verification	DERl	Digital Evidence Reliability
DFEW	Digital Forensics Expert Witness	DEP	Digital Evidence Proportionality

APPENDIX H: HM-DEAA CASE STUDIES — ADMISSIBILITY OF DIGITAL EVIDENCE

This appendix provides a template of the questionnaire that was administered to judges for the case study analysis of judicial cases considered and presented in Chapter 9. Judges were asked to identify the assessment criteria and questions and also allocate scores to each of the determinants. In order to ensure the judges understood the meaning and judicial significance of the various determinants, the researcher explained the principles underlying the scoring to the judges before they completed the questionnaire. Results from the case studies are discussed in Chapter 9.

HM-DEAA CASE STUDIES — ADMISSIBILITY OF DIGITAL EVIDENCE

INTRODUCTION:

Antwi-Boasiako and Venter (2017) has introduced a Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA) as the foundation of establishing digital evidence admissibility in criminal proceedings. The HM-DEAA is a model that integrates both technical and legal requirements to determine the admissibility of digital evidence in legal proceedings. The research is part of ongoing efforts to standardise digital forensics especially as it relates to digital evidence admissibility in judicial proceedings. A survey has already been conducted to validate the various technical and legal requirements. These determinants constitute the backbone of the HM-DEAA model. The request to participate in this research is part of case studies into the application of the HM-DEAA on judicial cases that have already been adjudicated by competent courts. The objective is to further establish the scientific foundations of the

HM-DEAA model. The Researcher will follow up with you to further discuss the HM-DEAA model and its application in judicial proceedings.

A. **BACKGROUND OF RESPONDENT** (kindly provide your background information)

SN	**Item**	**Response**
1	Job Title	
2	Summary of Job Role	
3	Brief Experience with Digital Evidence in Criminal Proceedings	
4	Geographical Region/Country	

B. **CASE BRIEF** (Provide a summary of the case which has already been adjudicated by the court including a brief description of the case, typology of digital evidence presented, criminal charges presented against the suspect (s), specific domestic legislations applied, etc.)

C. **DETERMINANT ASSESSMENT** (Complete the table below with the score assigned to each of the Determinants below as well as specific criteria/key questions considered in attributing the score to a particular determinant. Refer to Guidance Note A, B and C for further details and explanations on the *A. Determinant B. Assessment Score C. Assessment Criteria/Questions* respectively*.*

SN	Determinant	Assessment Score (1–5)	Assessment Criteria/Questions
1	Digital Forensics Model		• • •
2	Forensic Tools		
3	Chain of Custody		
4	Forensic Analyst Competency		
5	Digital Forensics Lab		
6	Technical Integrity Verification		
7	Digital Forensics Expert Witness		
8	Digital Forensics Report		
9	Legal Authorisation		
10	Digital Evidence Relevance		
11	Digital Evidence Authenticity		
12	Digital Evidence Integrity		
13	Digital Evidence Reliability		
14	Digital Evidence Proportionality		

D. **JUDICIAL DECISION** (Provide feedback on judgement delivered and any key considerations (relative to digital evidence or otherwise) by the Judge/Jury in arriving at the decision in the case.

E. **ADJUDICATION** (How do you consider the judgement/sentence delivered by the Judge/Jury in the case? Kindly tick one of the boxes below:

Minimum Sentence		Average Sentence		Maximum Sentence	

F. **JUDGEMENT DOCUMENT** (Can you respectfully provide a copy of the judgement document covering the case, if available under permissible disclosure? Please attach a copy to your completed form.)

GUIDANCE NOTE A: *Determinant Score Assessment*

Score	Description
1	LOWEST SCORE — Determinant met the lowest judicial requirements/expectations/assessment benchmarks. Thus, the required digital forensics requirements/expectations were mostly not adopted/followed in the case.
2	The Determinant met the minimum judicial requirements/expectations/assessment benchmarks. Thus, some minimum requirements were met but such requirements were below the average expected based on the assessment.
3	The Determinant met average judicial requirements/expectations/assessment benchmarks. This implies the determinant in question met half of the requirements based on the assessment.
4	The Determinant is considered above average in meeting the judicial requirements/expectations/assessment benchmarks. This implies the determinant in question exceeded the average expectations but did not meet the highest score based on the assessment.
5	HIGHEST SCORE — The Determinant met the highest judicial requirements/expectations/assessment benchmarks. All the known digital forensics requirements/expectations were adopted/followed in the case.

GUIDANCE NOTE B*: Summary Description of Determinants*

SN	Determinant	Determinant Description (Summary)
1	Digital Forensics Model/Approach	Whether the digital evidence under consideration was obtained through an appropriate digital forensics approach or procedure relative to the collection, processing and presentation of the evidence.
2	Digital Forensic Tools	Whether the digital evidence under consideration was obtained with an appropriate digital forensics tool (software or hardware) for collection, processing and presentation of the evidence.
3	Chain of Custody	Whether the digital evidence under consideration was obtained through sufficient and scientifically acceptable processes, procedures and activities involved in the preservation of the integrity of digital evidence.
4	Forensic Analyst Competency	Whether the digital evidence under consideration was processed by Analyst with acceptable qualification and experience in the collection, processing and presentation of the evidence.
5	Digital Forensics Lab	Whether the digital evidence under consideration was processed in a sound digital forensics laboratory environment, capable of guaranteeing a quality digital forensics work especially in the preservation, acquisition, processing and storage of the evidence.
6	Technical Integrity Verification	Whether the digital evidence under consideration was obtained with the use of adequate technical controls and measures (such as use of Write Blockers, Hash Values, etc.) in order to guarantee the integrity of the evidence.

SN	Determinant	Determinant Description (Summary)
7	Digital Forensics Expert	Whether the digital evidence under consideration was substantiated by adequate delivery of an opinion of a technical expert witness (if required).
8	Digital Forensics Report	Whether the digital evidence under consideration was presented in a form or a manner that was acceptable by the court.
9	Legal Authorisation	Whether the legal requirement or basis for searching, seizing and analysing devices or computer systems for digital evidence was met.
10	Digital Evidence Relevance	Whether the digital evidence under consideration was capable of successfully proving or disproving the case before the court.
11	Digital Evidence Authenticity	Whether the digital evidence under consideration was capable of establishing the facts in a way that could not be disputed by the court.
12	Digital Evidence Integrity	Whether the digital evidence under consideration was complete and unaltered.
13	Digital Evidence Reliability	Whether the digital evidence under consideration did not manifest any doubt in terms of its reliability by the court.
14	Digital Evidence Proportionality	Whether the digital evidence under consideration was based on only the information or electronic data that the law had authorised to be accessed.

GUIDANCE NOTE C: *Assessment Criteria/Questions*

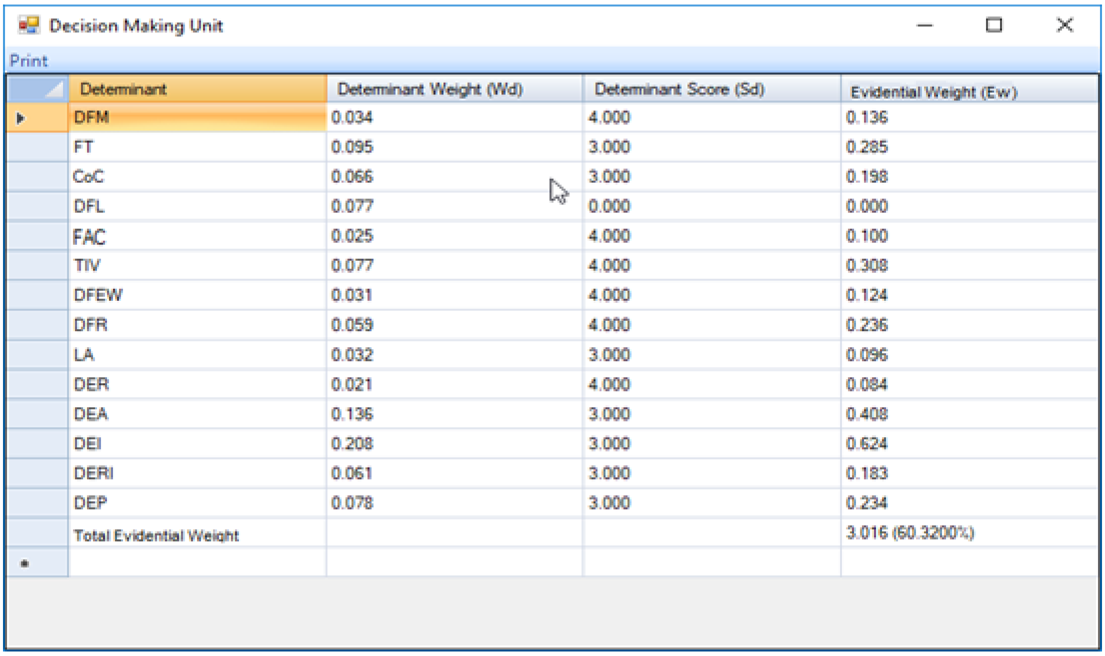
These are the considerations for allocating a score to a particular Determinant based on the Determinant meeting specific judicial requirements and assessment benchmarks. For example, in assessing the score of the Digital Forensics Tool Determinant, the following specific questions are taken into consideration (the list is not exhaustive).

Digital Forensics Tool — Assessment Criteria/Questions

- Which tool was used for forensic examination?
- Was the digital forensics tool used licensed?
- Has the tool used been tested/validated? By which body/institution?
- Has the tool been previously used in a similar case in another court, either in Ghana or in a similar legal jurisdiction?
- Is the tool open-source or proprietary?
- Are there any impacts of the tool used on the digital evidence processed?
- Does the tool have any recorded error rate?
- What is the level of acceptance of the tool among digital forensic examiners and researchers?
- Any scientific publication(s) on the tool?
- Other -

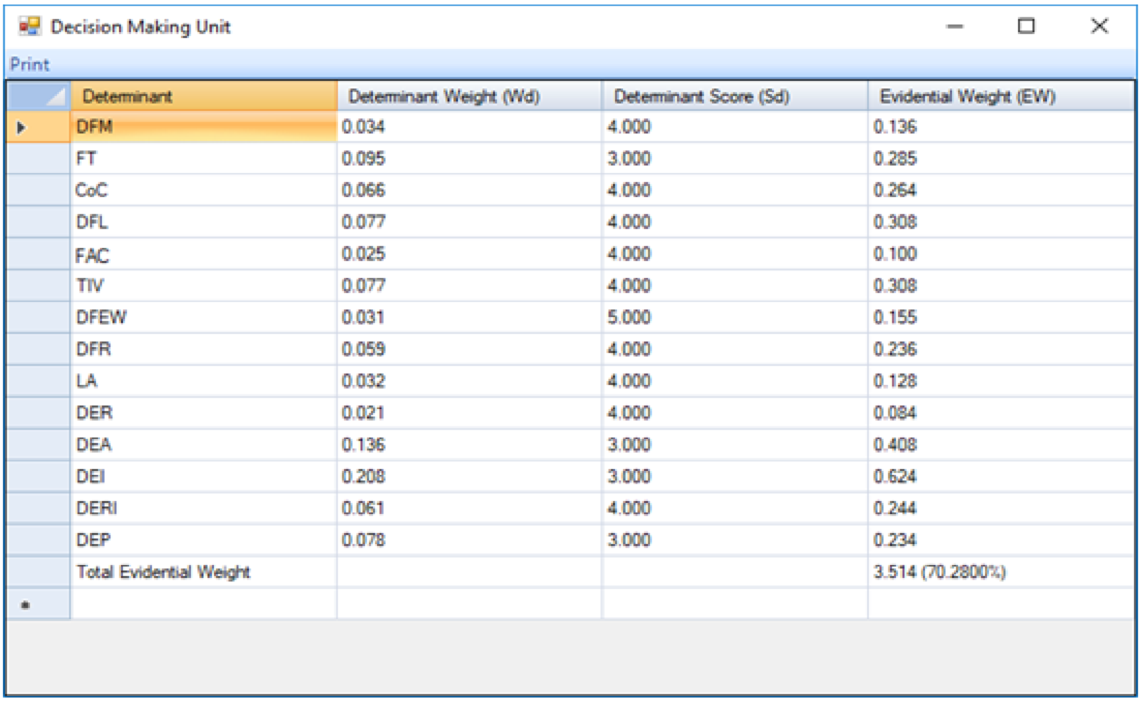
APPENDIX I: DETERMINANT WEIGHT OF CASES (CASE 1 TO CASE 10)

This appendix provides screenshots from the HM-DEAA ExP system, covering determinant weights obtained from the ten (10) judicial cases that were presented and discussed in Chapter 9.



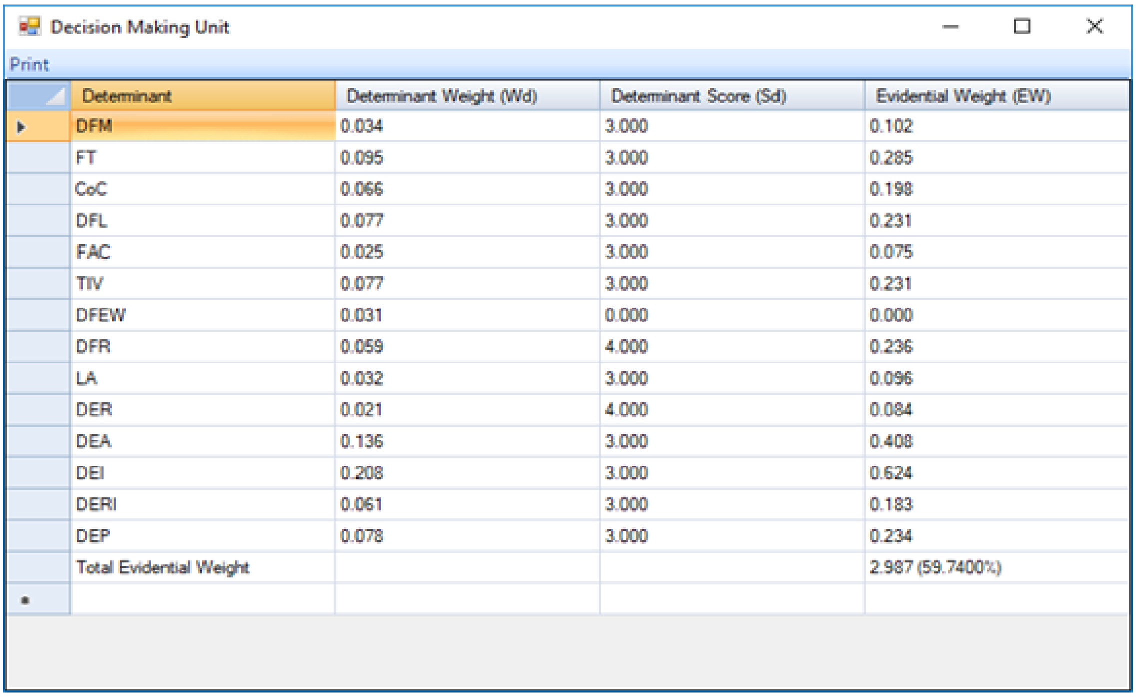
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (Ew)
DFM	0.034	4.000	0.136
FT	0.095	3.000	0.285
CoC	0.066	3.000	0.198
DFL	0.077	0.000	0.000
FAC	0.025	4.000	0.100
TIV	0.077	4.000	0.308
DFEW	0.031	4.000	0.124
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.016 (60.3200%)

Figure I.1 Determinant Weight for Case 1 using HM-DEAA ExP



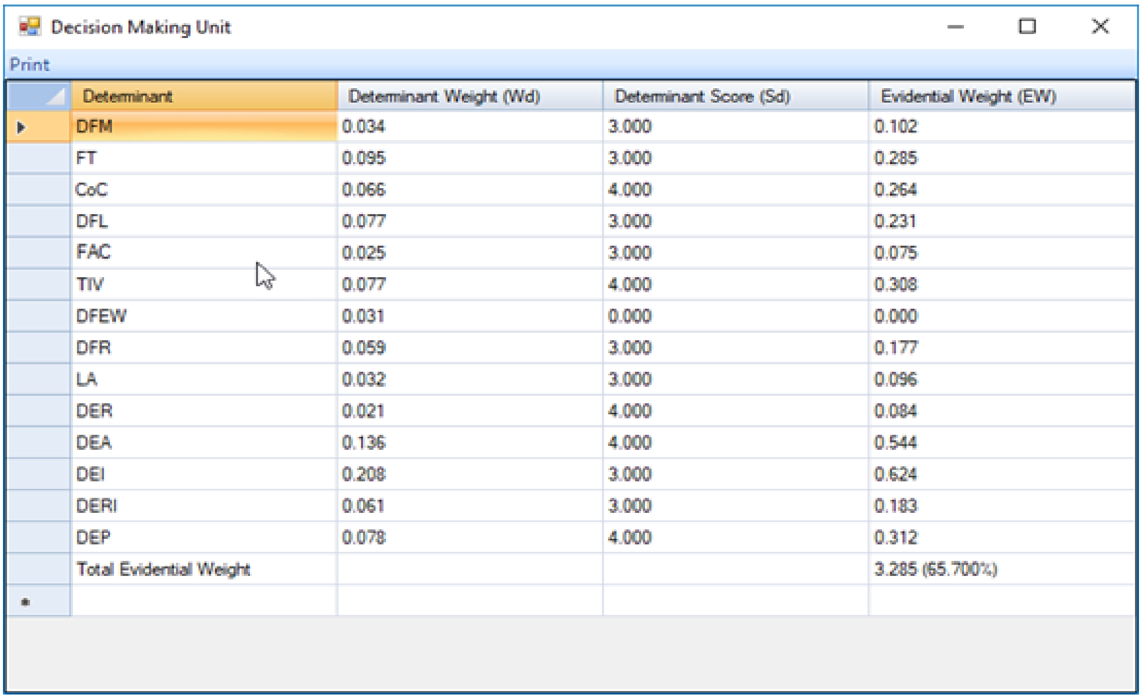
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	4.000	0.136
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	4.000	0.308
FAC	0.025	4.000	0.100
TIV	0.077	4.000	0.308
DFEW	0.031	5.000	0.155
DFR	0.059	4.000	0.236
LA	0.032	4.000	0.128
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	4.000	0.244
DEP	0.078	3.000	0.234
Total Evidential Weight			3.514 (70.2800%)

Figure I.2 Determinant Weight for Case 2 using HM-DEAA ExP



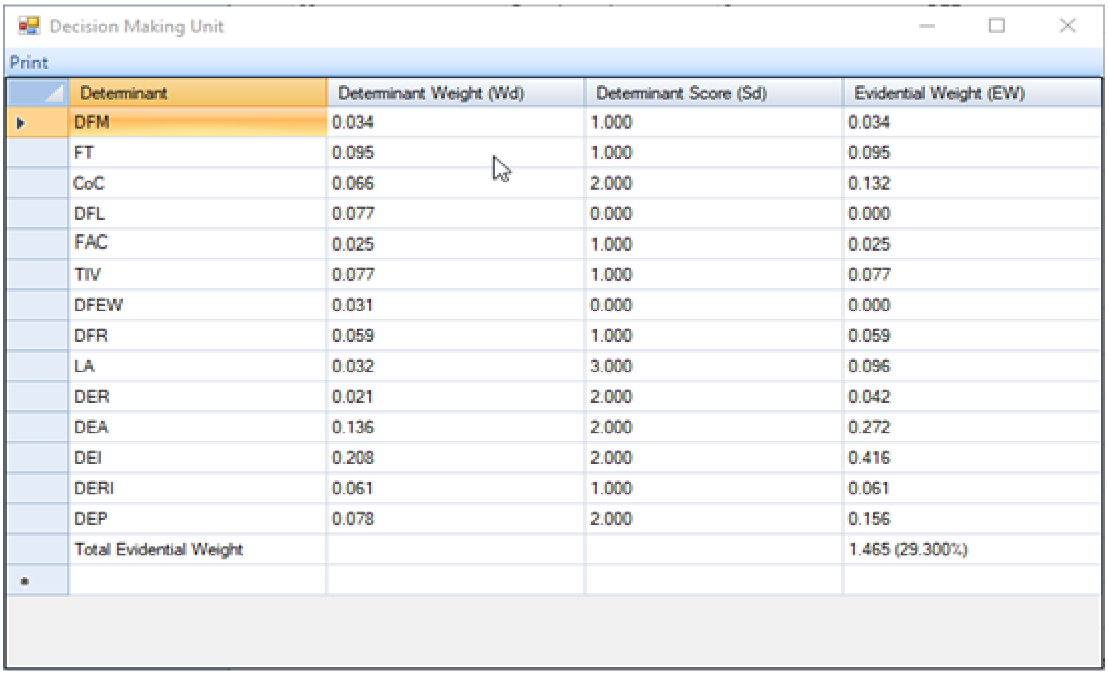
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	3.000	0.198
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	3.000	0.231
DFEW	0.031	0.000	0.000
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			2.987 (59.7400%)

Figure I.3: Determinant Weight for Case 3 using HM-DEAA ExP



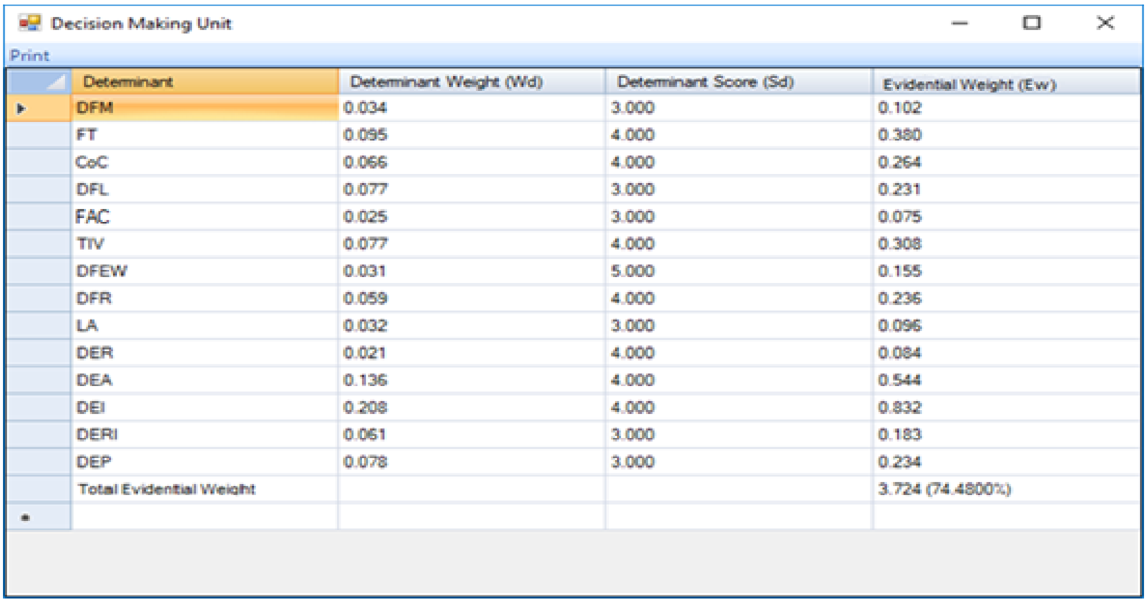
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	0.000	0.000
DFR	0.059	3.000	0.177
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	4.000	0.544
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	4.000	0.312
Total Evidential Weight			3.285 (65.700%)

Figure I.4: Determinant Weight for Case 4 using HM-DEAA ExP



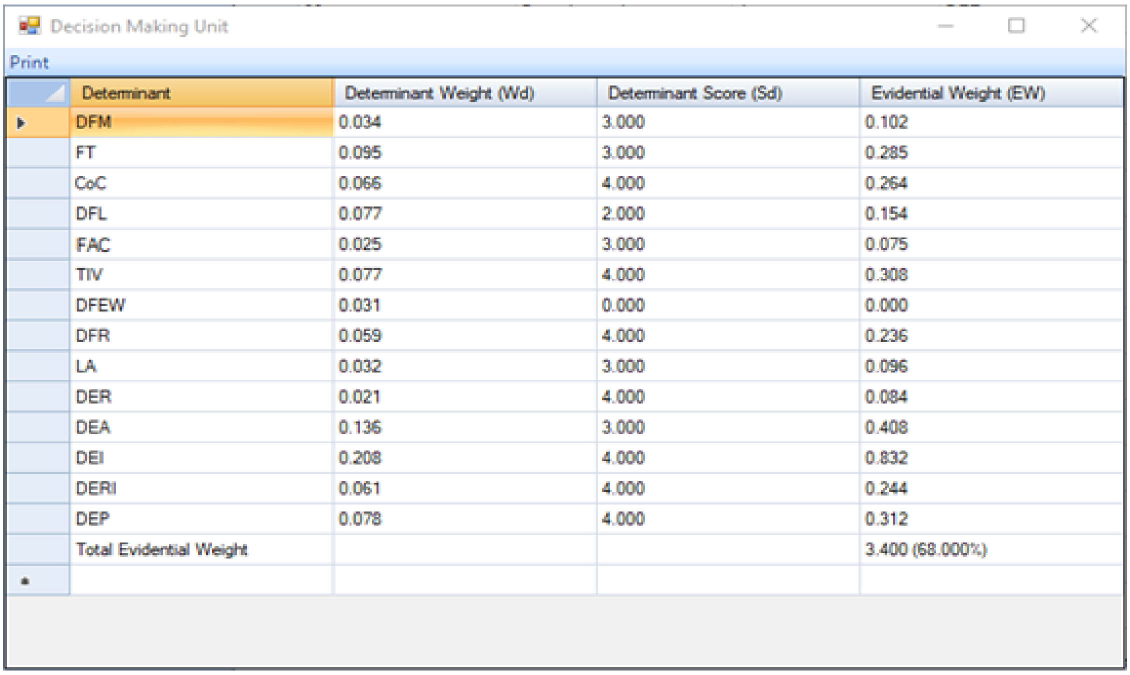
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	1.000	0.034
FT	0.095	1.000	0.095
CoC	0.066	2.000	0.132
DFL	0.077	0.000	0.000
FAC	0.025	1.000	0.025
TIV	0.077	1.000	0.077
DFEW	0.031	0.000	0.000
DFR	0.059	1.000	0.059
LA	0.032	3.000	0.096
DER	0.021	2.000	0.042
DEA	0.136	2.000	0.272
DEI	0.208	2.000	0.416
DERI	0.061	1.000	0.061
DEP	0.078	2.000	0.156
Total Evidential Weight			1.465 (29.300%)

Figure I.5: Determinant Weight for Case 5 using HM-DEAA ExP



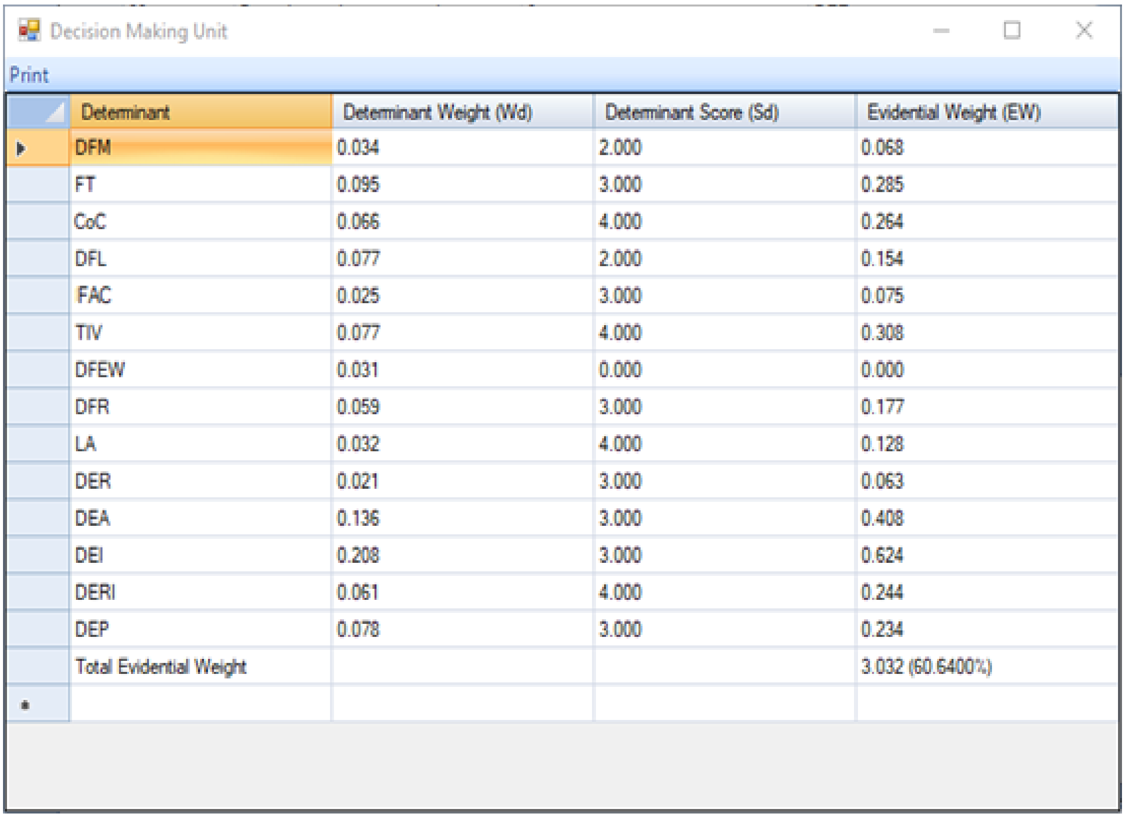
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (Ew)
DFM	0.034	3.000	0.102
FT	0.095	4.000	0.380
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	5.000	0.155
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	4.000	0.544
DEI	0.208	4.000	0.832
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.724 (74.4800%)

Figure I.6: Determinant Weight for Case 6 using HM-DEAA ExP



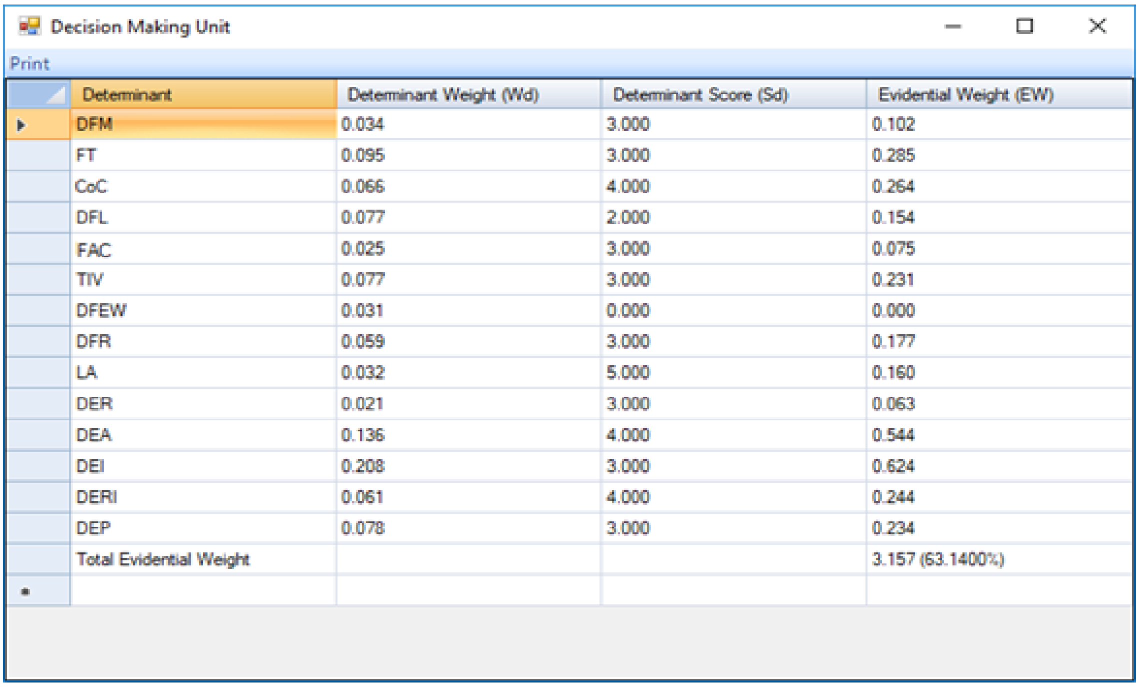
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	2.000	0.154
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	0.000	0.000
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	4.000	0.832
DERI	0.061	4.000	0.244
DEP	0.078	4.000	0.312
Total Evidential Weight			3.400 (68.000%)

Figure I.7: Determinant Weight for Case 7 using HM-DEAA ExP



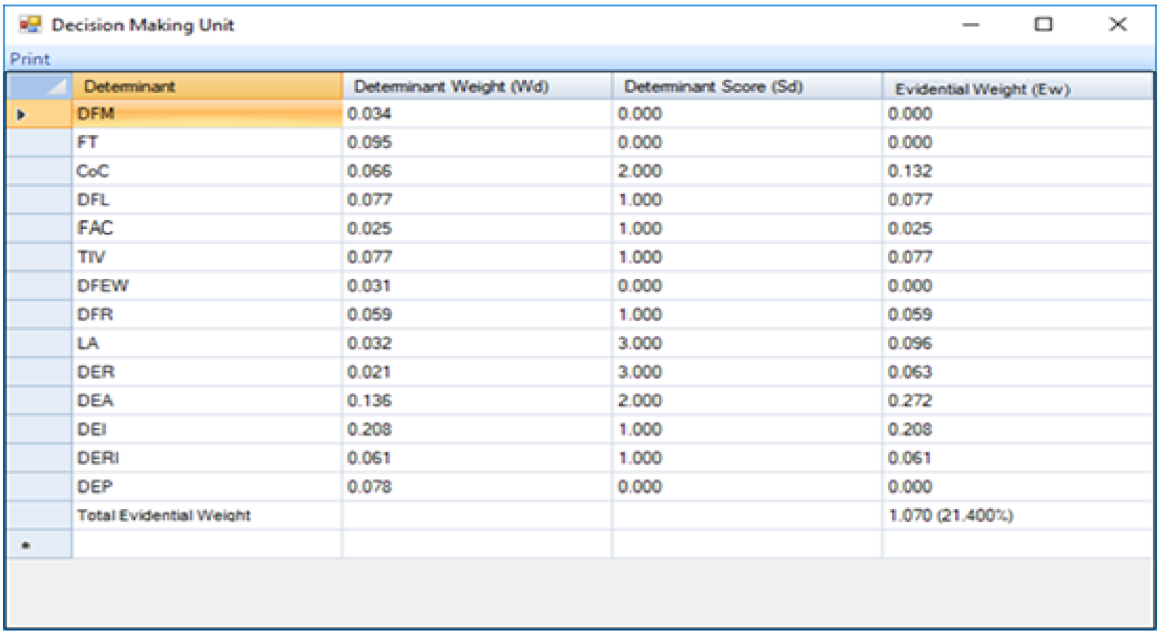
Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	2.000	0.068
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	2.000	0.154
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	0.000	0.000
DFR	0.059	3.000	0.177
LA	0.032	4.000	0.128
DER	0.021	3.000	0.063
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	4.000	0.244
DEP	0.078	3.000	0.234
Total Evidential Weight			3.032 (60.6400%)

Figure I.8: Determinant Weight for Case 8 using HM-DEAA ExP



Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (EW)
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	2.000	0.154
FAC	0.025	3.000	0.075
TIV	0.077	3.000	0.231
DFEW	0.031	0.000	0.000
DFR	0.059	3.000	0.177
LA	0.032	5.000	0.160
DER	0.021	3.000	0.063
DEA	0.136	4.000	0.544
DEI	0.208	3.000	0.624
DERI	0.061	4.000	0.244
DEP	0.078	3.000	0.234
Total Evidential Weight			3.157 (63.1400%)

Figure I.9: Determinant Weight for Case 9 using HM-DEAA ExP

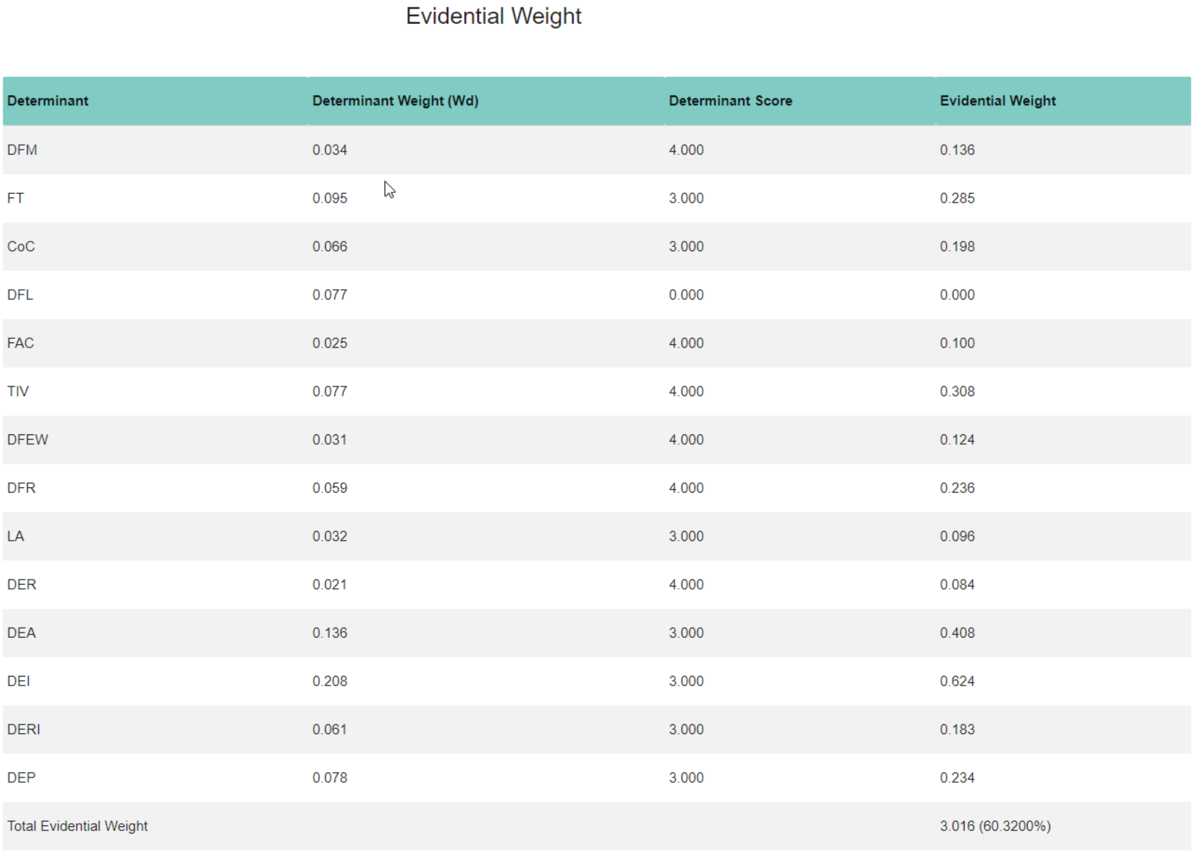


Determinant	Determinant Weight (Wd)	Determinant Score (Sd)	Evidential Weight (Ew)
DFM	0.034	0.000	0.000
FT	0.095	0.000	0.000
CoC	0.066	2.000	0.132
DFL	0.077	1.000	0.077
FAC	0.025	1.000	0.025
TIV	0.077	1.000	0.077
DFEW	0.031	0.000	0.000
DFR	0.059	1.000	0.059
LA	0.032	3.000	0.096
DER	0.021	3.000	0.063
DEA	0.136	2.000	0.272
DEI	0.208	1.000	0.208
DERI	0.061	1.000	0.061
DEP	0.078	0.000	0.000
Total Evidential Weight			1.070 (21.400%)

Figure I.10: Determinant Weight for Case 9 using HM-DEAA ExP

APPENDIX J: REPORT ON CASES (CASE 1 TO CASE 10) FROM THE HM-DEAA ExP

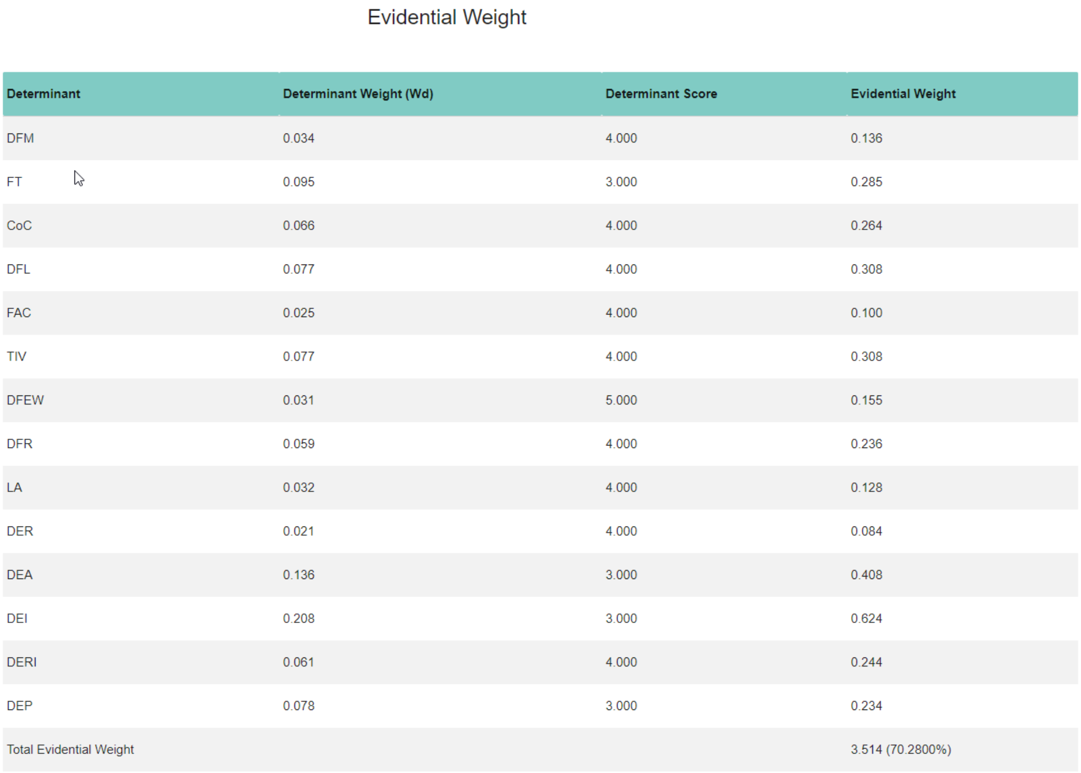
This appendix provides screenshots of reports generated by the HM-DEAA ExP system covering the ten (10) judicial cases presented and discussed in Chapter 9. The HM-DEAA model was applied on the ten (10) cases as part of the evaluation of the model introduced in the thesis.



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	4.000	0.136
FT	0.095	3.000	0.285
CoC	0.066	3.000	0.198
DFL	0.077	0.000	0.000
FAC	0.025	4.000	0.100
TIV	0.077	4.000	0.308
DFEW	0.031	4.000	0.124
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.016 (60.3200%)

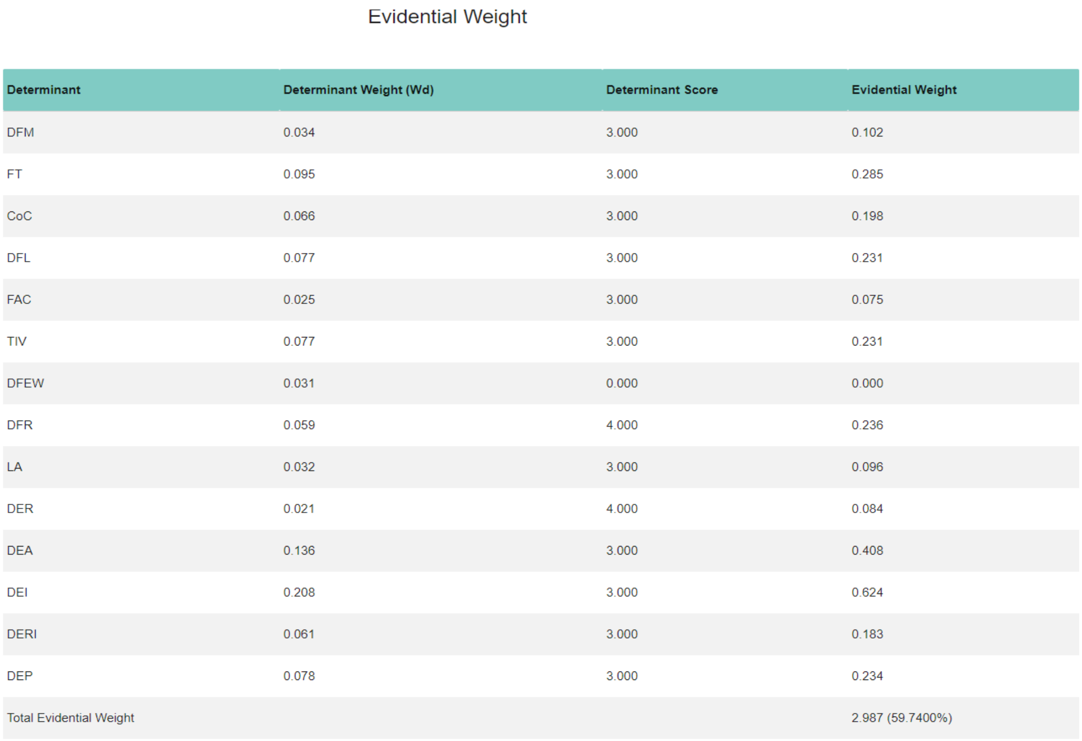
Figure J.1: Report on Case 2 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	4.000	0.136
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	4.000	0.308
FAC	0.025	4.000	0.100
TIV	0.077	4.000	0.308
DFEW	0.031	5.000	0.155
DFR	0.059	4.000	0.236
LA	0.032	4.000	0.128
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	4.000	0.244
DEP	0.078	3.000	0.234
Total Evidential Weight			3.514 (70.2800%)

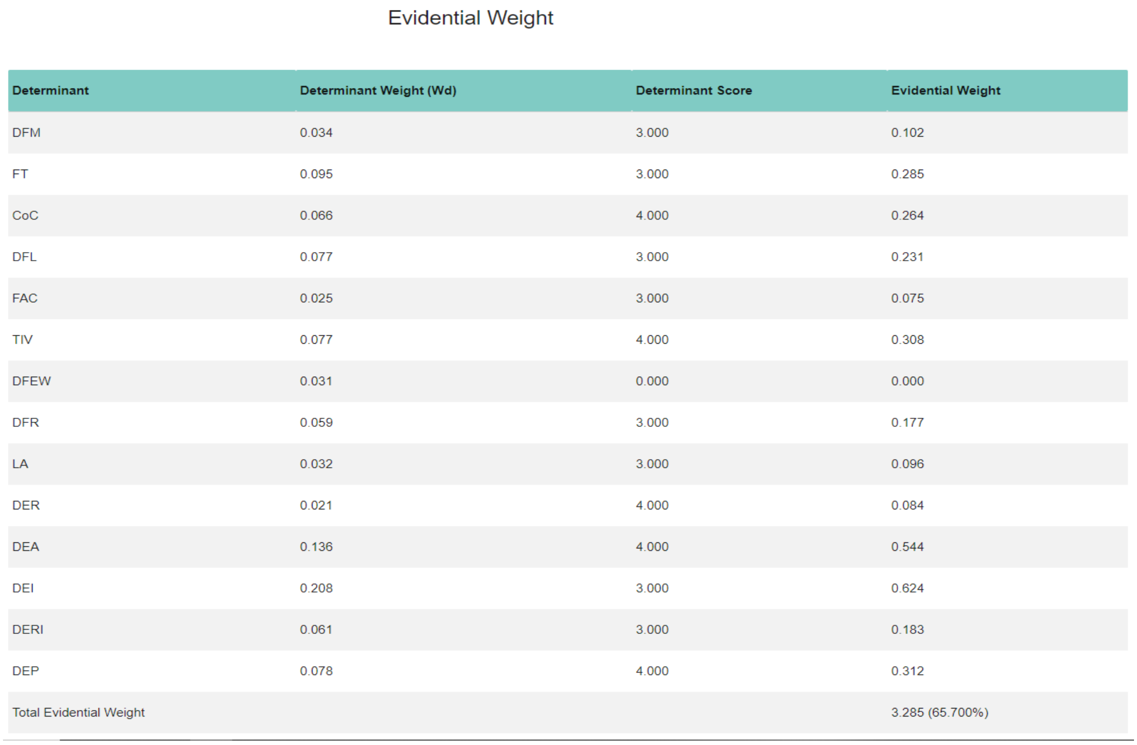
Figure J.2: Report on Case 2 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	3.000	0.198
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	3.000	0.231
DFEW	0.031	0.000	0.000
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			2.987 (59.7400%)

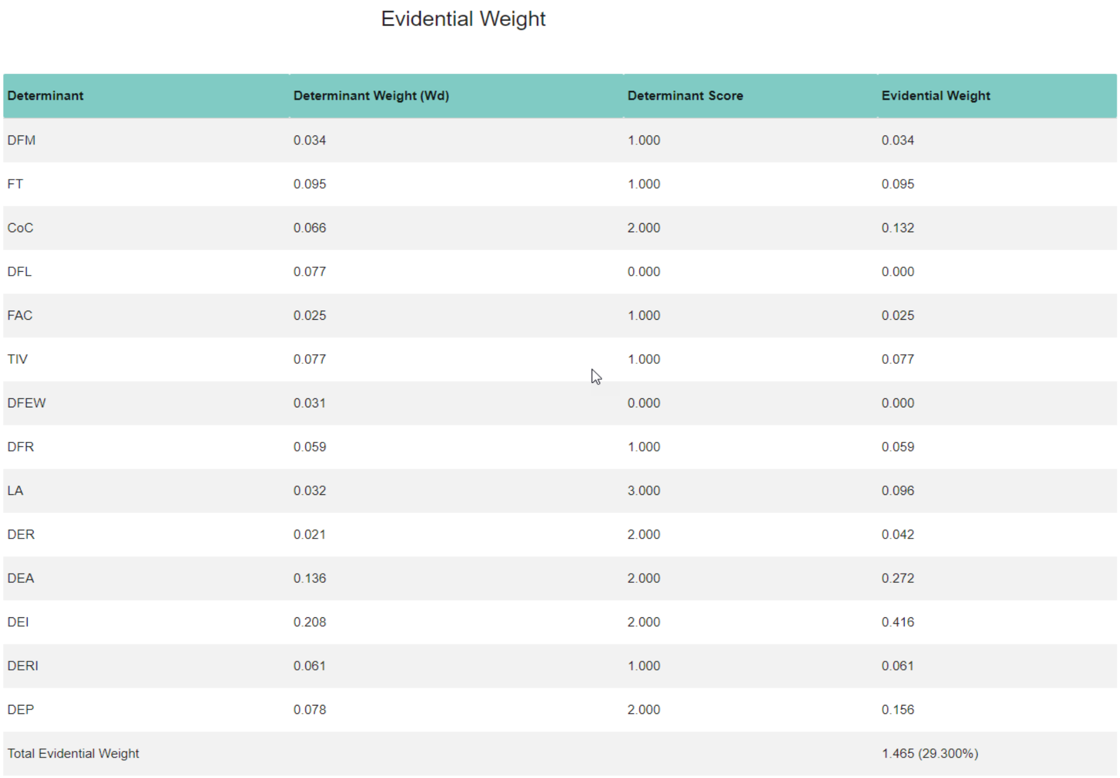
Figure J.3: Report on Case 3 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	0.000	0.000
DFR	0.059	3.000	0.177
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	4.000	0.544
DEI	0.208	3.000	0.624
DERI	0.061	3.000	0.183
DEP	0.078	4.000	0.312
Total Evidential Weight			3.285 (65.700%)

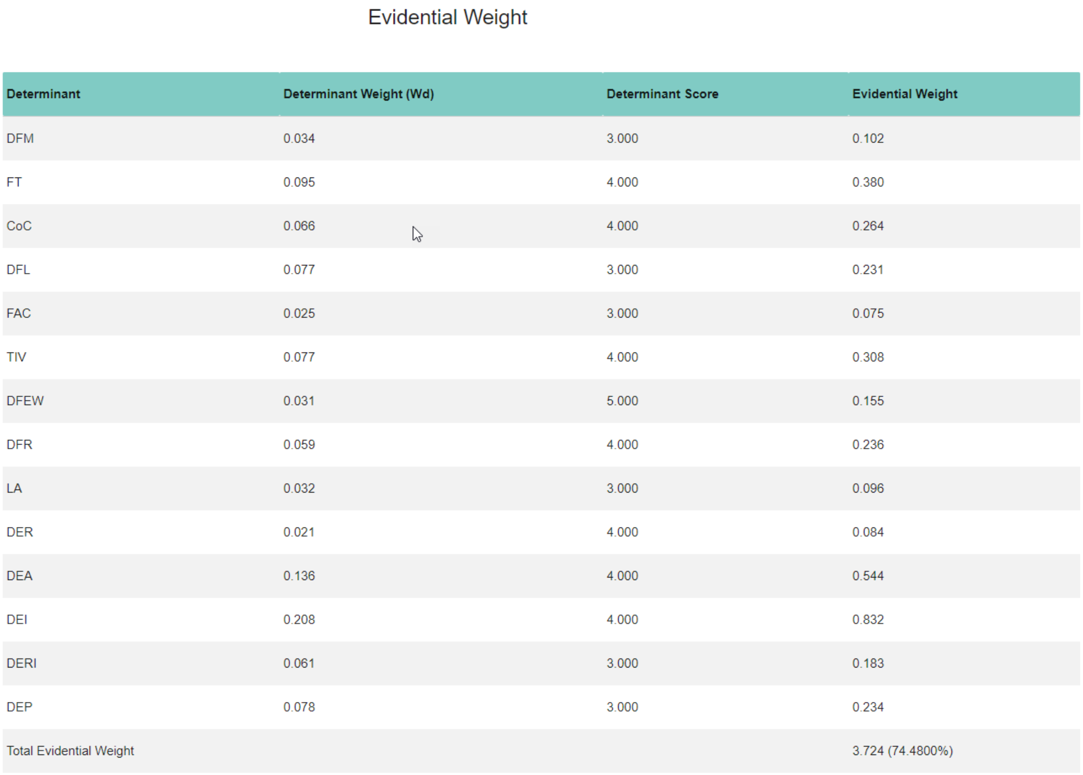
Figure J.4: Report on Case 4 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	1.000	0.034
FT	0.095	1.000	0.095
CoC	0.066	2.000	0.132
DFL	0.077	0.000	0.000
FAC	0.025	1.000	0.025
TIV	0.077	1.000	0.077
DFEW	0.031	0.000	0.000
DFR	0.059	1.000	0.059
LA	0.032	3.000	0.096
DER	0.021	2.000	0.042
DEA	0.136	2.000	0.272
DEI	0.208	2.000	0.416
DERI	0.061	1.000	0.061
DEP	0.078	2.000	0.156
Total Evidential Weight			1.465 (29.300%)

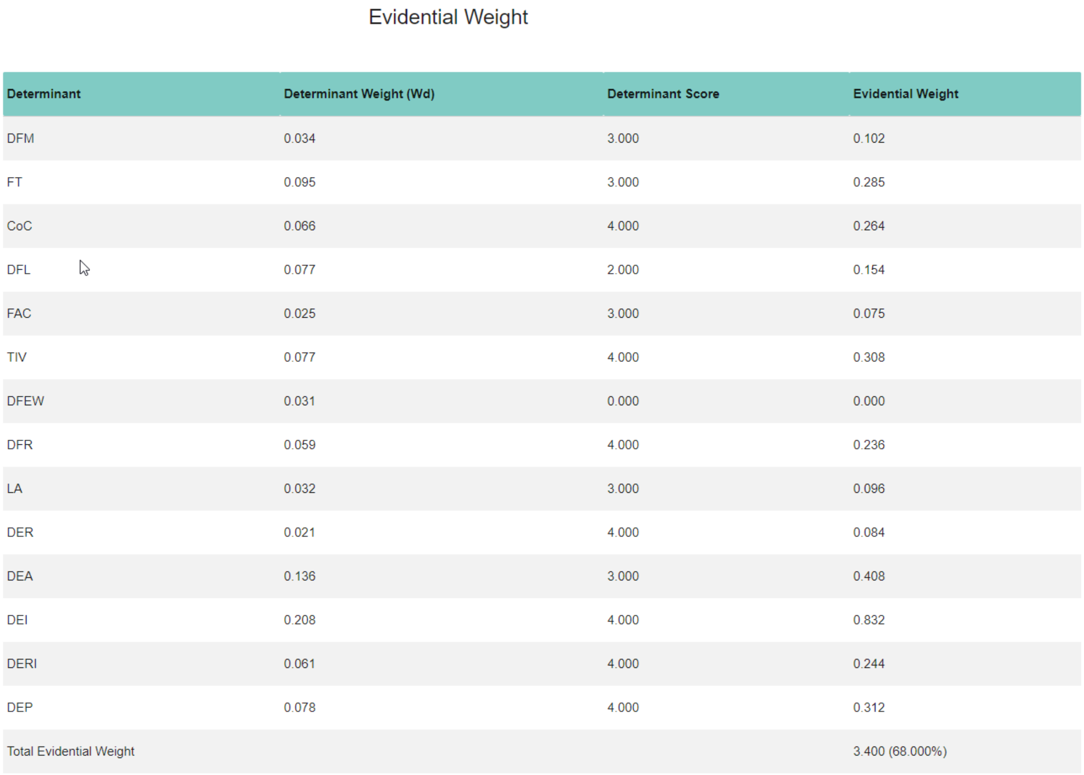
Figure J.5: Report on Case 5 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	4.000	0.380
CoC	0.066	4.000	0.264
DFL	0.077	3.000	0.231
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	5.000	0.155
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	4.000	0.544
DEI	0.208	4.000	0.832
DERI	0.061	3.000	0.183
DEP	0.078	3.000	0.234
Total Evidential Weight			3.724 (74.4800%)

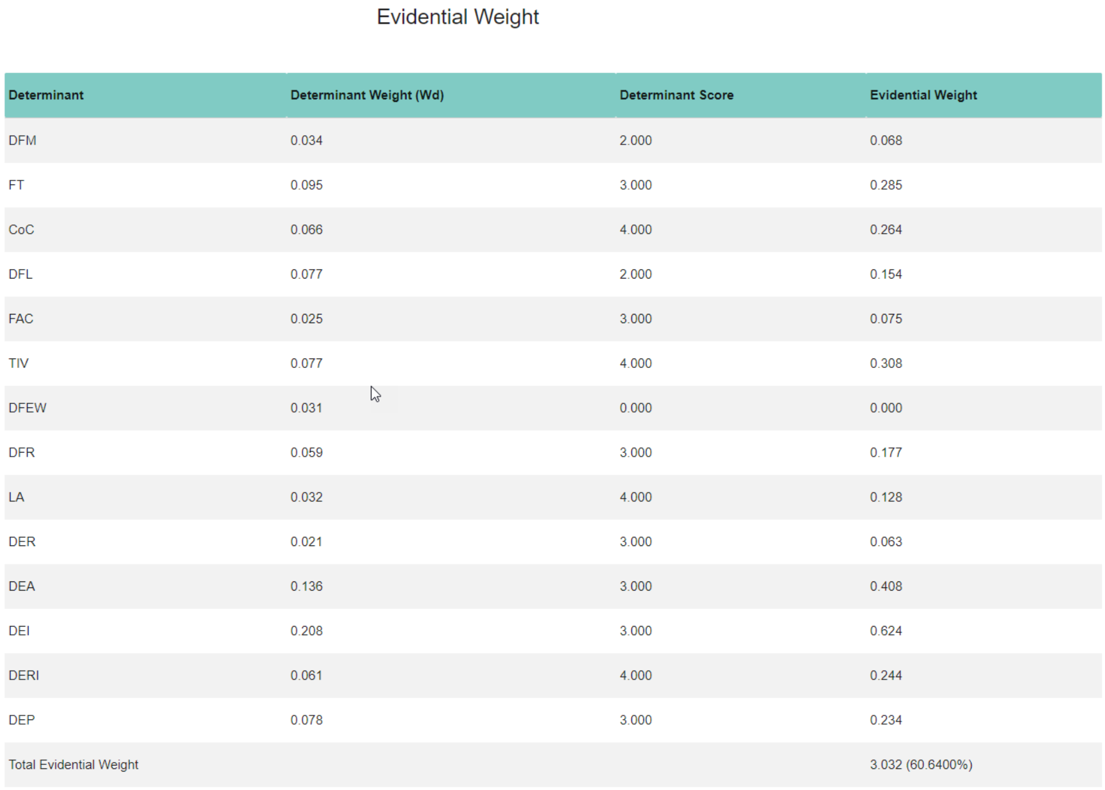
Figure J.6: Report on Case 6 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	2.000	0.154
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	0.000	0.000
DFR	0.059	4.000	0.236
LA	0.032	3.000	0.096
DER	0.021	4.000	0.084
DEA	0.136	3.000	0.408
DEI	0.208	4.000	0.832
DERI	0.061	4.000	0.244
DEP	0.078	4.000	0.312
Total Evidential Weight			3.400 (68.000%)

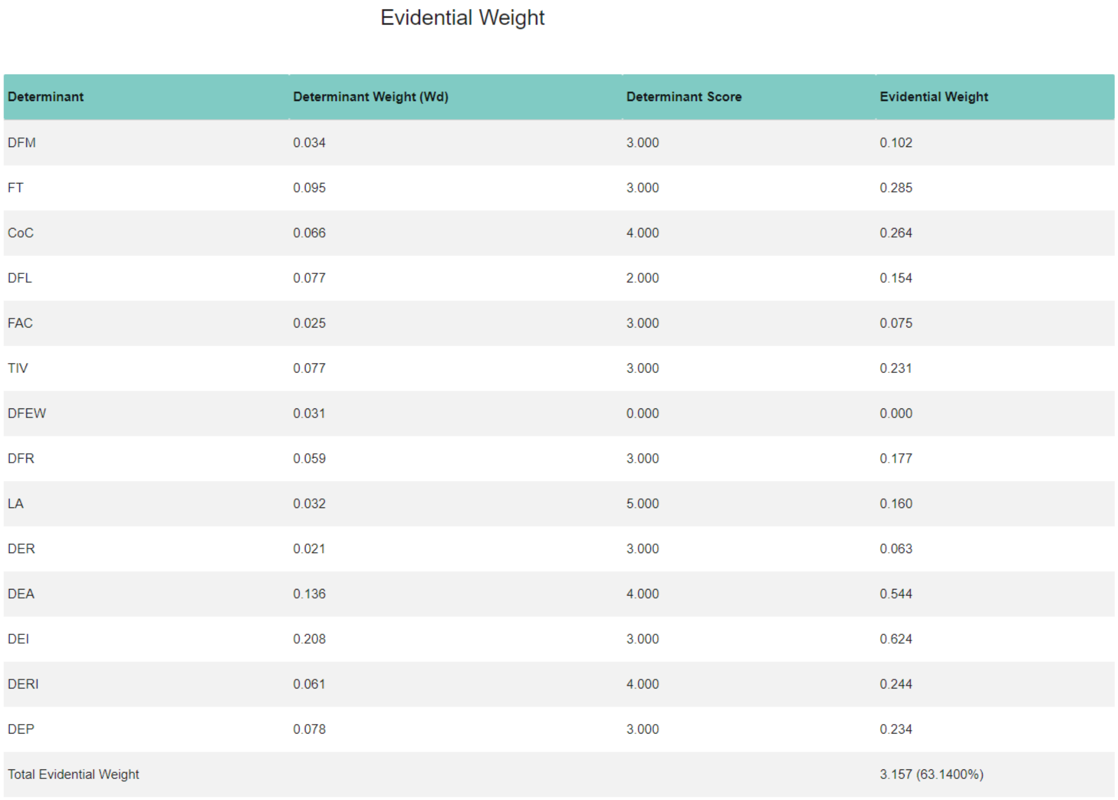
Figure J.7: Report on Case 7 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	2.000	0.068
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	2.000	0.154
FAC	0.025	3.000	0.075
TIV	0.077	4.000	0.308
DFEW	0.031	0.000	0.000
DFR	0.059	3.000	0.177
LA	0.032	4.000	0.128
DER	0.021	3.000	0.063
DEA	0.136	3.000	0.408
DEI	0.208	3.000	0.624
DERI	0.061	4.000	0.244
DEP	0.078	3.000	0.234
Total Evidential Weight			3.032 (60.6400%)

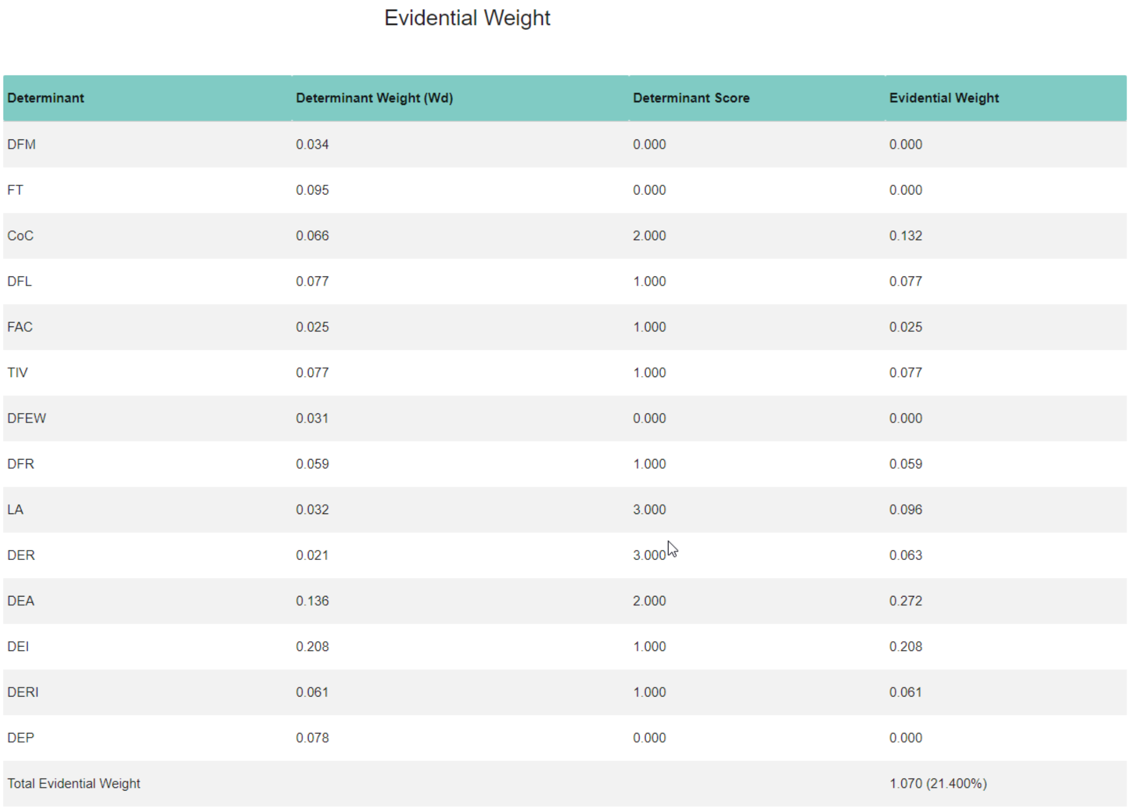
Figure J.8: Report on Case 8 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	3.000	0.102
FT	0.095	3.000	0.285
CoC	0.066	4.000	0.264
DFL	0.077	2.000	0.154
FAC	0.025	3.000	0.075
TIV	0.077	3.000	0.231
DFEW	0.031	0.000	0.000
DFR	0.059	3.000	0.177
LA	0.032	5.000	0.160
DER	0.021	3.000	0.063
DEA	0.136	4.000	0.544
DEI	0.208	3.000	0.624
DERI	0.061	4.000	0.244
DEP	0.078	3.000	0.234
Total Evidential Weight			3.157 (63.1400%)

Figure J.9: Report on Case 9 from the HM-DEAA ExP



Evidential Weight

Determinant	Determinant Weight (Wd)	Determinant Score	Evidential Weight
DFM	0.034	0.000	0.000
FT	0.095	0.000	0.000
CoC	0.066	2.000	0.132
DFL	0.077	1.000	0.077
FAC	0.025	1.000	0.025
TIV	0.077	1.000	0.077
DFEW	0.031	0.000	0.000
DFR	0.059	1.000	0.059
LA	0.032	3.000	0.096
DER	0.021	3.000	0.063
DEA	0.136	2.000	0.272
DEI	0.208	1.000	0.208
DERI	0.061	1.000	0.061
DEP	0.078	0.000	0.000
Total Evidential Weight			1.070 (21.400%)

Figure J.10: Report on Case 10 from the HM-DEAA ExP

APPENDIX K: HM-DEAA ExP SYSTEM SOURCE CODES

This appendix provides the source codes for the HM-DEAA ExP System. The HM-DEAA ExP is a software application developed to automate the HM-DEAA model introduced in the thesis. Further details pertaining to the software are discussed in Chapter 8.

Main Program

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace HM_DEAAExpertSystem
{
  static class Program
  {
    /// <summary>
    /// The main entry point for the application.
    /// </summary>
    [STAThread]
    static void Main()
    {
      Application.EnableVisualStyles();
      Application.SetCompatibleTextRenderingDefault(false);
      Application.Run(new ScoringForm());
    }
  }
}
```

Module: Get Determinants

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace HM_DEAAExpertSystem.Modules
{
   public class Determinant
   {
      public int ID { get; set; }
      public string Name { get; set; }
      public decimal DeterminantScore { get; set; }

      public override string ToString()
      {
         return this.Name;
      }

   }
}
```

Module: Get Determinant Assessments Questions

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace HM_DEAAExpertSystem.Modules
{
    public class Question
    {
        public int ID { get; set; }
        public string Quest { get; set; }

        public Determinant Determinant { get; set; }
        public override string ToString()
        {
            return this.Quest;
        }

        public static Question RetrieveQuestion(int id)
        {
           var questions = new Database.QuestionDB().Read(string.Format("select * from
questions where id={0}",id));
            return questions[0]; //return the first question, only one question will be
returned anyway.

        }
    }

}
```

Module: Determinant Score

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace HM_DEAAExpertSystem.Modules
{
    class DeterminantScore
    {
        public string Question { get; set; }
        public decimal Score { get; set; }
    }
}
```

Module: Determinant Scoring

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace HM_DEAAExpertSystem.Modules
{

     public struct Score
      {
         public string Question;
         public decimal Scored;
         public Determinant Determinant;
      }
}
```

Module: Result

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;

namespace HM_DEAAExpertSystem.Modules
{
   public class Result
   {
      public int ID { get; set; }
      public List<Question> Questions { get; set; }
      public List<Determinant> Determinants { get; set; }
      public List<decimal> Score { get; set; }
      public int Case_Id { get; set; }
   }
}
```

Module: Generate Report

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.IO;
using System.Diagnostics;
using System.Windows.Forms;
using DevComponents.AdvTree;

namespace HM_DEAAExpertSystem.Modules
{
  class GenerateReport
  {

    private const string _TableRowScoring = @"{{TableRowScoring}}";
    private const string _TableRowEvidentialWeight =
@"{{TableRowEvidentialWeight}}";

    private const string _CompanyName = @"{{CompanyName}}";
    private const string _ReportType = @"{{ReportType}}";

    private const string _TableHeader = @"{{TableHeader}}";
    public static DateTime DateFrom { get; set; }
    public static DateTime DateTo { get; set; }

    private DataGridViewRowCollection _ScoringDataGridViewRowsCollection;
    private DataGridViewRowCollection
_EvidentialWeightDataGridViewRowsCollection;
    const string TITLE = "HM-DEAA ExP System";

    public GenerateReport(DataGridViewRowCollection scoringataGridViewRows,
DataGridViewRowCollection evidentialWeightDataGridViewRows)
    {
      _ScoringDataGridViewRowsCollection = scoringataGridViewRows;
      _EvidentialWeightDataGridViewRowsCollection =
evidentialWeightDataGridViewRows;

    }
    private string TableRow()
    {

      string tableRow = "";

      foreach (DataGridViewRow row in _ScoringDataGridViewRowsCollection)
      {
```

Decision making Unit

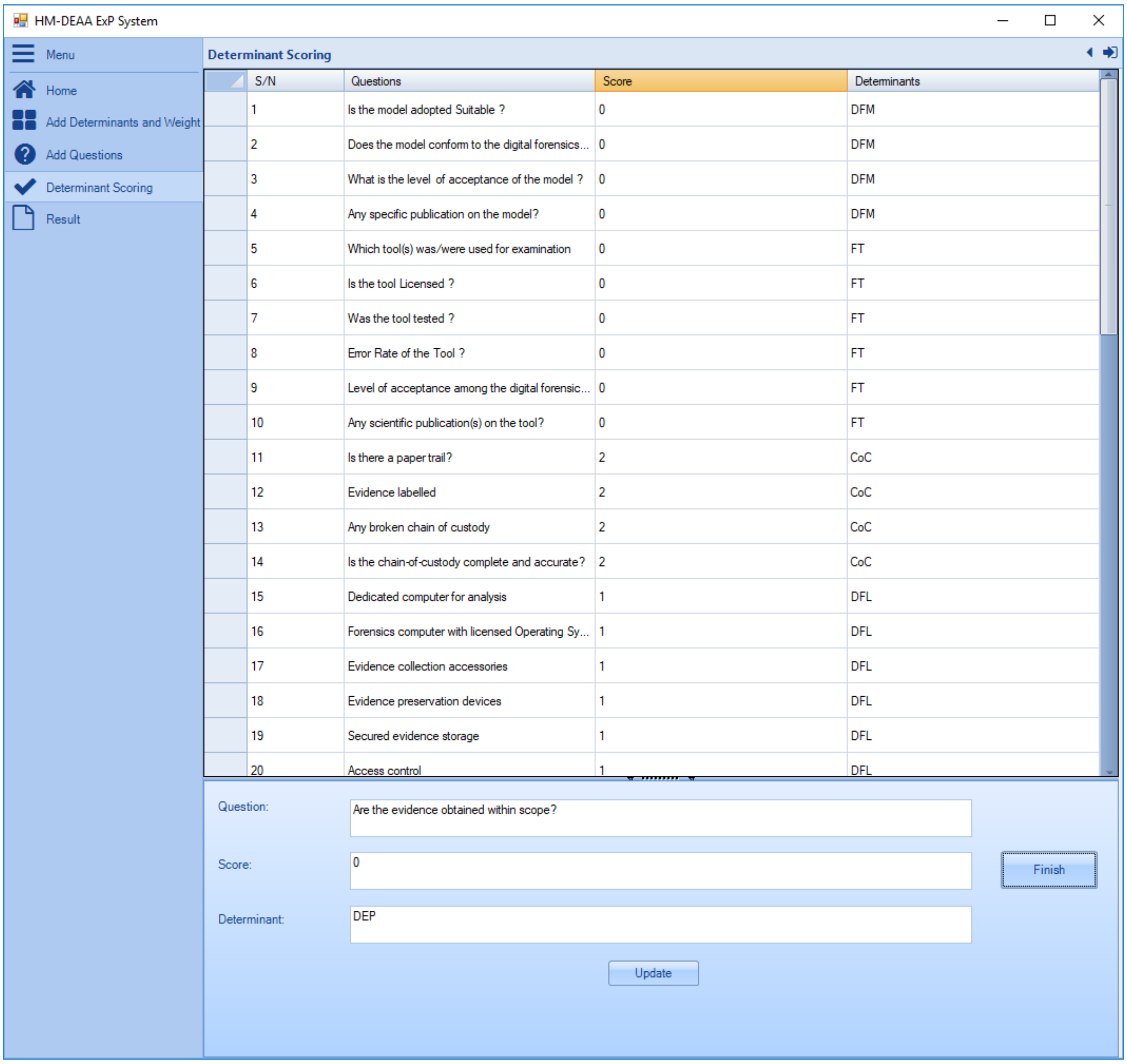
```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

using DevComponents.DotNetBar;
using HM_DEAAExpertSystem.Modules;

namespace HM_DEAAExpertSystem
{
    public partial class DecisionMakingUnit : Office2007Form
    {
        public Result result { get; set; }
        public DataGridViewRowCollection _ScoringRows { get; set; }
        public DecisionMakingUnit()
        {
            InitializeComponent();
        }

        public DecisionMakingUnit(List<Score> scores, DataGridViewRowCollection
scoringRows) : this()
        {
            List<string> processedDeterminants = new List<string>();
            DataGridViewTextBoxCell totalweightedValueCell = new
DataGridViewTextBoxCell();
            DataGridViewTextBoxCell totalweightedLabelCell = new
DataGridViewTextBoxCell();
            DataGridViewRow _row = null;
            _ScoringRows = scoringRows;

            foreach (var score in scores)
            {

                if (processedDeterminants.Contains(score.Determinant.Name)) continue;

                 _row = new DataGridViewRow();
                DataGridViewTextBoxCell determinantName = new
DataGridViewTextBoxCell();
                DataGridViewTextBoxCell determinantWeight = new
DataGridViewTextBoxCell();
                DataGridViewTextBoxCell determinantScore = new
DataGridViewTextBoxCell();
                DataGridViewTextBoxCell weightedValue = new DataGridViewTextBoxCell();
```

Scoring Form

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using DevComponents.DotNetBar;
using HM_DEAAExpertSystem.Modules;

namespace HM_DEAAExpertSystem
{
  public partial class ScoringForm :  Office2007Form
  {

    private UserLoginForm _UserLoginForm { get; set; }

    public ScoringForm()
    {
      InitializeComponent();
    }

    public ScoringForm(UserLoginForm userLoginForm):this()
    {
      _UserLoginForm = userLoginForm;

    }

    #region Determinants

    private void btnAddDeterminantsCategory_Click(object sender, EventArgs e)
    {
      var determinant_name = txtDeterminant.Text.Trim();
      var determinant_score = Convert.ToDecimal(txtEvidentialWeight.Text.Trim());

      Modules.Determinant determinant = new Modules.Determinant() {Name=
determinant_name, DeterminantScore= determinant_score };
      determinant = new Database.Repository().Add(determinant);

      DataGridViewRow row = new DataGridViewRow();
      row.Tag = determinant;

      DataGridViewTextBoxCell cell_determinant_name = new
DataGridViewTextBoxCell();
      cell_determinant_name.Value = determinant_name;
```

APPENDIX L: HM-DEAA ExP SYSTEM INTERFACE

This appendix provides a screenshot of the HM-DEAA ExP system interface. Details about the software are presented in Chapter 8.



Determinant Scoring

S/N	Questions	Score	Determinants
1	Is the model adopted Suitable ?	0	DFM
2	Does the model conform to the digital forensics...	0	DFM
3	What is the level of acceptance of the model ?	0	DFM
4	Any specific publication on the model?	0	DFM
5	Which tool(s) was/were used for examination	0	FT
6	Is the tool Licensed ?	0	FT
7	Was the tool tested ?	0	FT
8	Error Rate of the Tool ?	0	FT
9	Level of acceptance among the digital forensic...	0	FT
10	Any scientific publication(s) on the tool?	0	FT
11	Is there a paper trail?	2	CoC
12	Evidence labelled	2	CoC
13	Any broken chain of custody	2	CoC
14	Is the chain-of-custody complete and accurate?	2	CoC
15	Dedicated computer for analysis	1	DFL
16	Forensics computer with licensed Operating Sy...	1	DFL
17	Evidence collection accessories	1	DFL
18	Evidence preservation devices	1	DFL
19	Secured evidence storage	1	DFL
20	Access control	1	DFL

Question: Are the evidence obtained within scope?

Score: 0

Determinant: DEP

Figure L.1: HM-DEAA ExP System Interface

APPENDIX M: PUBLISHED AND PENDING PAPERS FROM THE RESEARCH

This appendix provides details of published and pending papers from the research.

Published Papers:

1. A. Antwi-Boasiako and H. Venter, *A Model for Digital Evidence Admissibility Assessment*, in Advances in Digital Forensics XIII, pp. 23 to 38, 2017.
2. A. Antwi-Boasiako and H. Venter*, Implementing the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA),* Proceedings of the 15th Annual IFIP WG 11.9 International Conference on Digital Forensics, Florida, United States of America, 2019

Submitted Paper:

1. A. Antwi-Boasiako and H. Venter, *An Expert System for Implementing the Harmonised Model for Digital Evidence Admissibility Assessment (HM-DEAA)*, The International Journal of Digital Forensics and Incident Response, 2019.