# Case Study Research as a Method for Digital Forensic Evidence Examinations

by

Oluwasayo Oyeyemi Oyelami

Submitted in fulfilment of the requirements for the degree
Master of Science (Computer Science)
in the Faculty of Engineering, Built Environment and Information Technology
University of Pretoria, Pretoria

November 2018

Publication data:

Oluwasayo Oyeyemi Oyelami. Case Study Research as a Method for Digital Forensic Evidence Examinations, University of Pretoria, Department of Computer Science, Pretoria, South Africa, November 2018.

Electronic, hyperlinked versions of this dissertation are available online, as Adobe PDF files, at:

http://icsa.cs.up.ac.za/

http://upetd.up.ac.za/UPeTD.htm

# Case Study Research as a Method for Digital Forensic Evidence Examinations

by

Oluwasayo Oyeyemi Oyelami
E-mail: sayo.oyelami@gmail.com

## Abstract

At the heart of any forensic science discipline, there is the need to ensure that the method applied in the discipline is based on a valid scientific method. The aim of any forensic examination is to make verifiable and consistent inferences about phenomena with high certainty. The highest state of inference is determining causality. In science, two methods that can be applied in digital forensic examinations are experimentation and case studies. Experimentation is a well-tested scientific method used for a whole range of scientific studies, but there are situations where it is not always possible to carry out experiments. In these cases, the case study method offers a suitable alternative approach to examining phenomena. Though case study research is very popular in the social sciences and not widely used in the natural sciences. it is accepted as a valid method and applying this method in examining digital occurrences may produce insightful results. This research work examines the suitability of case study research as a scientific foundation for digital forensics. The research aims to show that case study method provides a scientific foundation for digital forensics and a suitable adapted method of case study research would be applicable in examining digital evidence.

**Keywords:** Forensic science, digital forensics, digital examination, digital evidence, case study research, case study.

**Supervisor** : Prof. M. S. Olivier
**Department** : Department of Computer Science
**Degree** : Master of Science

“Sometimes it is the people no one imagines anything of who do the things that no one can imagine”

Alan Turing

“Thinking is allowed”

Unknown

*To my Dad, Abraham Oyebisi Oyelami,*

*for always having my back and for believing in me*

# Acknowledgements

I sincerely appreciate the following people for their unparalleled support and assistance throughout the writing of this dissertation:

- Professor Martin S. Olivier, for your academic guidance and for being an excellent life coach.
- My mother, Mojisola Oyelami, for your patience, love and prayers.
- My brothers, Sogo Oyelami, Segun Oyelami and Seyi Oyelami, for your encouragement through the years.
- My colleagues, for their commitment to knowledge sharing.
- ICSA research group, for the insightful academic travels and support.

# Contents

# Chapter 1

# Introduction

> *In regard to legal matters the requirement to prove a case beyond reasonable doubt and the weight of evidence presented before the court are crucial factors in the determination of the outcome of a case. In a criminal case where the method applied in examining evidence produced findings that favoured a guilty outcome and these findings are later proven to be faulty, the need to examine the reliability and adequacy of the methods applied in examining evidence becomes paramount.*

Most transactions today typically rely on the use of digital devices for seamless communication. Financial systems, industrial systems and world economies mainly rely on digital systems to work effectively. An individual previously could only engage in financial transactions by visiting a financial institution within specific hours; now, these transactions can be completed using a variety of internet-connected digital devices. It is no surprise that digital crimes have increased over the past decade mainly due to the widespread use of digital devices. Crimes such as financial fraud and identity theft have become synonymous with digital crimes. Cyber criminals are capable of breaching corporate IT infrastructure with malicious intent such as to cripple IT services, steal money, and exfiltrate sensitive data from vulnerable systems within the organisation. These cyber criminals, also known as adversaries, include script kiddies, crime syndicates as well as nation-state actors.

Unlike physical crimes, the nature of computer crimes allows the perpetrator to commit crimes without physically being at the crime scene. However, like physical crimes where investigators may find fingerprints, footprints, DNA samples as well as other physical evidence, digital crimes generate footprints also known as artefacts or traces within affected systems and devices at the scene of the crime. As physical crimes sometimes leave artefacts that can be investigated and traced back to the perpetrators or employed in narrowing down the suspects to a list of possibilities, traces found in digital crimes may also be useful in determining the actions executed by the perpetrators within the environment [31]. Determining these actions enable investigators to reconstruct plausible patterns of events and attribute events to sources or root causes.

In a digital investigation, traces can be found in different locations on a digital system. These include web browsers, system registry, computer servers, network systems, intrusion detection systems, firewall systems, personal computer systems and mobile devices. These devices and systems logs are preserved as evidence and examined to determine the events of the crime. Digital examinations also enable a forensic examiner to demonstrate a consistent reconstruction of the crime should the perpetrators be apprehended, and the case is examined by the courts. The handling and examination of evidence must, however, be done in a forensically sound manner to be accepted as evidence by the court.

Ultimately, the findings of a forensic examination will depend on how the evidence was obtained, its forensic soundness, the examination process, interpretation of the findings, and the probative value of the evidence before the court. A forensically sound examination process ensures that the findings of the examination have a high level of certainty.

## 1.1 Motivation

*To provide scientifically based facts applied in a legal or justice system to support and uphold the law.* This is the goal of forensic science. This goal is achieved through the application of science and law to legal matters in the determination of truth. A landmark National Academy of Science report [36] noted that the court's reliance on forensic science poses important questions about forensic science disciplines. These questions include the following:

- How scientific are the processes used in carrying out a forensic inquiry?
- How certain are the findings of a forensic inquiry?
- How can the findings of a forensic inquiry be shown to be reliable and consistent with respect to the goals of the inquiry?

The need to ensure the certainty of the findings of a forensic inquiry and the ability to demonstrate the method applied in obtaining these findings is scientific is a critical requirement in most forensic science disciplines that claim to be scientific. This is the motivation for this research: To demonstrate the application of science in digital forensics and validate the findings made in a forensic examination.

## 1.2 Context of this Research

In applying a scientific approach to digital forensics, the examination of evidence provides a suitable point where science can be introduced. The aim of forensic examinations is to identify, examine and attribute phenomena to plausible causes. A cause produces its effect. The effect is the phenomenon observed. The cause may be intermediate causes or root causes. The determination of the cause of a phenomenon, the sound reconstruction of the pattern of events, the consistency established by the causal relationships demonstrated between the causes and effects observed using a logical and methodological approach, satisfy the requirement for a scientifically sound approach for the examination of digital evidence.

In science, two methods that can be applied in achieving this aim are experimentation and case-study research. The use of experiments in examining phenomena is well established and has been applied in a wide range of scientific studies. Experiments, however, are also limited since when complex phenomena are examined by means of experiments, the factors and conditions that formed the phenomenon cannot all be considered at once. There are also situations where it would be unthinkable to carry out experiments as it may have disastrous effects within the environment. In other situations where experiments are possible, one may not wish to carry out experiments due to factors such as prohibitive costs. In these situations, there is a need to examine the phenomenon using a different method.

The application of case study research, though not widely applied in the natural sciences, offers a viable alternative method to experimentation. Case studies are suitable for examining a complex phenomenon within its real-world context taking into consideration all the factors and conditions that formed the phenomenon. Case studies very often do not have a disastrous impact when applied in examining an unforgiving phenomenon. Its application may even reveal more findings than an experiment can provide.

The application of case study research to forensic examinations is non-existent and the only research done in this area of study was carried out by Oyelami and Olivier [44] [43]. There is therefore the need for a formal approach for conducting forensic examinations in digital forensics using case studies. This research aims to examine how this can be done: by applying the case study method to digital examinations, an inherent logical approach is applied that ensures the consistency of findings and demonstrates the application of science to the forensic examination.

Yin [65] provides a systematic approach to examining phenomena. This approach is well established in the social sciences having been shown to be sound with Yin's seminal publication, "Case Study Research and Applications", is in its 6th edition [66].

## 1.3 Problem Statement

This research applies Yin's case study approach to digital forensic examinations and demonstrates the method can be suitably applied in determining and establishing causes within a digital forensic investigation as well as validating the findings of the digital investigation.

In order to address the research problem, several sub-problems need to be addressed. These are:

- To provide an analysis of the state of the field of digital forensics in the context of forensic science disciplines;

- To apply case study as a scientific method to forensic examinations specifically in the field of digital forensics;

- To show that case study method can be suitably used in examining forensic evidence;
- To strongly align the case study method to current practices in digital forensics; and
- To demonstrate the scientific status of digital forensics using case study research.

## 1.4 Contributions

This dissertation makes the following novel contributions to the field of digital forensics:

- An analysis of the state of the field of digital forensics in the context of forensic science disciplines.
- The "discovery" of a scientific method that closely aligns with digital forensics.
- The introduction of case study research as a scientific method for digital forensics.
- The application of case study research to examine digital evidence.
- The determination that case study research is more closely aligned with digital forensics than experimentation.
- The determination that case study research validates and extends what is currently achieved in digital forensics.

## 1.5 Dissertation Outline

The layout of the dissertation is provided below with a brief overview of each chapter of the dissertation.

- **Chapter 2** focuses on the relationship between forensic science and the law and the intricacies that outline this relationship. It further provides a discussion on the state of forensic science disciplines with emphasis on digital forensics.

- **Chapter 3** provides an overview and discussion which aims at investigating peer-reviewed research carried out in the field of digital forensics with a focus on methods geared towards examination of digital evidence using a scientific approach.
- **Chapter 4** develops a conceptual framework for examining digital evidence using Yin's case-study method.
- **Chapter 5** develops a model for applying case studies to forensic examinations. It further provides a critical discussion on several key aspects of the model such as validity, addressing alternative plausible explanations, establishing a web of consistency, causality and demonstrating logical reconstructions.
- **Chapter 6** provides further discussions on the model concepts and its applications within a digital forensic context.
- **Chapter 7** concludes the dissertation and provides a list of possible future work.

The following appendix containing a list of relevant information are included for quick referencing purposes:

- **Appendix A** lists the publications derived from this work.

# Chapter 2

# Forensic Science and the Law

Science is an enduring search for truth [33]. This search has been shown to be a far-reaching and continuous process. It is then not surprising that the definition of science has seen many modifications with no generally accepted definition in the scientific community. While science has lacked a consensus on a general definition, the goal of science has been widely accepted, is firm and unwavering.

The goal of science is to discover truths that explain real-world occurrences based on valid empirical and logical (including mathematical) deductions [39]. Law, on the other hand considers disputes with the goal to determine the facts of a legal case. A valid claim is a fact, which is regarded as the "truth". In a situation where two opposing claims are valid, the weight or probative strength of the claims enables the court to determine the outcome of the case. The claim having more support using different valid sources of evidence is considered as having greater probative strength than the opposing claim.

The stronger claim is considered the greater "truth" and is accepted as fact while the other opposing claim is disproved or set-aside by the court due to its lesser probative strength. The need for law to ensure that its findings are based on facts aided the application of science to matters of law. This synergy inherently produced forensic science disciplines. The disciplines of forensic science are dedicated to the application of scientific techniques and principles for the determination of facts that are scientifically valid. The goal of forensic science is to provide scientifically based facts applied in a legal or justice system to support and uphold the law [36] [39] [44].

The rest of this chapter explores various aspects relevant to forensic science and is structured as follows: Section 2.1 provides an introduction to forensic science. Section 2.2 provides a brief description of forensic science disciplines. Section 2.3 provides a discussion on the impact of the forensic science on legal matters. Section 2.4 provides a discussion on the requirements for the legal admissibility of scientific evidence. Section 2.5 illustrates the scientific method. Section 2.6 provides a summary of the chapter.

## 2.1 What is Forensic Science

Forensic science is an intriguing subject, and its definition makes it even more intriguing. Several attempts to define forensic science have caused much heated debate through the years without producing a consensus or a generally accepted definition. The difficulty is occasioned by the challenge to define science itself. The definition for forensics on the other hand is very clear. The word *forensic* has at its origin, the notion of a *forum* - a place of public debate. This in contemporary practice would refer to a court of law. This definition does emphasize certain conclusions. *forensics* does not have the same meaning as *forensic science*. Olivier in [40] provides a definition for forensic science.

*Forensic science* is defined as the "application of science to answer questions that are of interest to matters of law".

The definition emphasises the need for the "application of science" where forensic enquiries are concerned. The challenge then is to determine what constitutes science and what is non-science? This is a hard question, one which has been reflected upon by scientists and philosophers over the years. This problem is known as the *demarcation* problem in the philosophy of science [28] [52]. Several criteria have been formulated to classify what can be construed as science and what is not science within what is termed as the demarcation criteria.

The following three demarcation criteria can be considered the most important landmarks in the philosophy of science [67] [39] [22]. The first is the notion of logical positivism. The notion of logical positivism was developed by a group known as the Vienna Circle [63] [15] [53]. The Vienna circle agreed that statements derived from mathematical and logical tautologies and empirically verifiable claims are considered meaningful and scientific while other claims are inherently unreliable or useless. The notion therefore requires that a claim must be backed by mathematical or logical reasoning and must be verifiable for it to be considered scientific. This criterion poses a requirement which most forensic science disciplines, except for DNA analysis, have failed to meet.

The second demarcation criterion is falsifiability. The falsifiability criterion was proposed by Karl Popper. Popper [48] [49] proposed that theoretical propositions or theories are regarded as scientific if they can be tested and are falsifiable. Falsifiability indicates that there are scientific tests that can be performed to demonstrate that these propositions are false. A falsified theory is replaced by a new theory which has not been falsified using the same or higher criteria despite numerous attempts to disprove the theory. Popper regarded falsifiability as both a necessary and a sufficient condition to confirm that any theory is scientific. Falsifiability as a necessary condition implies that for a theory to be considered scientific, scientific tests capable of falsifying the theory must have been applied to disprove the theory. Falsifiability as a sufficient condition implies that the repeated failed attempts to falsify a theory indicates that the theory is scientific and that once a theory has been falsified, it can no longer be deemed as scientific.

The third criterion is postpositivism or postempiricism proposed by Thomas Kuhn [27]. Kuhn described scientific activities as a puzzle-solving activity which involves the application of scientific paradigms in solving problems. A scientific paradigm which fails to solve a new problem is replaced with another paradigm which solves all the problems solved by the previous paradigm it replaced and the new problem encountered. [67] [39][22]

While the philosophy of science provides criteria for recognising science, the law also provides criteria for what can be accepted by the court as scientific evidence. A later section of this chapter discusses criteria for admissibility of scientific evidence in the court of law.

## 2.2 Categorisation of Forensic Science Disciplines

Forensic science encompasses a broad range of disciplines. These disciplines cover various aspects of forensic inquiries with varying scientific degree regarding general acceptability, reliability, techniques, methods, error rates, research and peer reviewed publications. Due to these distinctions, several forensic disciplines classified as forensic science disciplines lack the scientific underpinning to be considered as such. However, progress in science and research continue to impact on the state of several forensic science disciplines.

Several classifications have been proposed for forensic science disciplines [36] [35]. A recent classification by the United States National Institute of Science and Technology [37] classified forensic science disciplines into five general categories as shown below:

1. *BIOLOGY AND DNA* which include Biological Data Interpretation and Reporting, Biological Methods, and Wildlife Forensics

2. *CHEMISTRY AND INSTRUMENTAL ANALYSIS* which include Fire Debris and Explosives, Geological Materials, Gunshot Residue, Trace Materials, Seized Drugs and Toxicology

3. *CRIME SCENE AND DEATH INVESTIGATION* which include Anthropology, Disaster Victim Identification, Dogs and Sensors, Fire and Explosion Investigation, Medico-legal Death Investigation and Odontology

4. *DIGITAL AND MULTIMEDIA* which include Video and Imaging technology and Analysis, Speaker Recognition, Facial Recognition, and Digital Evidence

5. *PHYSICS AND PATTERN INTERPRETATION* which include Bloodstain Pattern Analysis, Firearms and Toolmarks, Footwear and Tyre, Forensic Document Examination and Friction Ridge

## 2.3 The Impact of Forensic Science on Legal Matters

The impact of forensic science on legal matters cannot be overemphasised. In determining the "truth" of a legal case, especially criminal cases, the court relies heavily on forensic science to make justified inferences regarding a case [39]. Records show that many people have been incarcerated based on evidence obtained from invalid application of science [51] [36]. Some of these court rulings have been overturned due to the results of scientific research from evidence analysis derived from DNA analysis. The impact of bad science cannot be estimated only in terms of the wasted years that the innocent spent in incarceration but also in the lack of trust in the courts and in the reliability of the methods employed in several forensic science disciplines.

The court's reliance on forensic science poses important questions such as: *"how scientific are the processes applied in carrying out a forensic enquiry?"*, *"how certain are we of the findings of a forensic enquiry?"*, *"how can we show that the findings of a forensic enquiry are reliable and consistent with the enquiry we are tasked to solve?"* [36]. These questions must be answered in scientific enquiries especially those requiring legal proceedings.

Much science precedes a forensic investigation. The National Academy of Sciences (NAS) report [36] noted that techniques such as DNA analysis, serology, forensic pathology, toxicology, chemical analysis and digital forensics are built on a scientific body of knowledge based on theory and research. The report [36] further concluded that, "With the exception of nuclear DNA analysis . . . no forensic method has been rigorously shown to have the capacity to consistently, and with a high degree of certainty, demonstrate a connection between evidence and a specific individual or source."

## 2.4 Requirements for Legal Admissibility of Scientific Evidence

The need to ensure that evidence that is accepted by the courts is scientific occasioned the need to fashion out rules for evidence admissibility. In the bid to validate scientific evidence before its admittance as evidence in court, tests covering several requirements have been proposed to satisfy the scientific admissibility of expert testimony. While various courts apply different approaches and strategies to determine evidence admissibility, the approach employed by the United States is widely discussed in the digital forensic literature and is therefore discussed in this research. Three standards discussed are the Frye standard, the Federal Rules of Evidence and the Daubert standard.

The first standard is the Frye test, also widely known as the general acceptance test. The Frye standard requires that scientific, technical or specialised knowledge must have general acceptance within the relevant scientific community for it to be considered acceptable by the courts. This implies that forensic evidence will only be admissible if it passes the general acceptance test. The general acceptance test provides that for an expert testimony or a technique to be admissible and considered reliable as scientific evidence, the technique applied must hold general acceptance within the relevant scientific community. To meet the Frye standard, the court must conclude that scientific evidence presented to the court applies generally accepted procedures, principles or techniques and that the validity of the evidence is supported by experts working in the relevant scientific field [13] [17].

The Frye standard originated from the Frye vs the United States case [13] where the discussion centred on the admissibility of polygraph tests as scientific evidence. In this case, the court noted the need for methods to employ the use of clearly defined experimental procedures based on a well-recognised scientific principle or discovery, and that the deductions made from using this method must have general acceptance in the scientific community from which it is derived [13].

The second standard is provided by the Federal Rules of Evidence (FRE) Rule 702 [25]. In 1975, the Federal Rules of Evidence took effect in US federal courts. Rule 702 which is part of the FRE replaced the Frye standard. The first version of the rule required that a scientific, technical or specialised knowledge provided by an expert witness qualified by knowledge, skill, experience, training, or education that can assist the court in understanding the evidence or determining facts was acceptable. Rule 702 to a degree lowered the requirement for “general acceptance” enforced by the Frye standard which it superseded [25].

The Federal Rules of Evidence Rule 702 provides key provisions for admission of expert testimony in court. The first provision required that the expert testimony must be backed by scientific knowledge which is grounded and derived from applying the scientific method. The second provision required that the expert testimony must assist the court in the determination of facts within the context of the case. The third provision required the judge to weigh the expert evidence and make a threshold determination on whether the evidence can be accepted as scientific or not based on whether the reasoning or methodology underlying the testimony is scientifically valid. These three key provisions weigh heavily when scientific evidence is considered for admissibility under Rule 702. It is noteworthy that Rule 702 did not include Frye's standard of general acceptance as a requirement for evidence admissibility by the court. [25].

The third standard for legal admissibility is the Daubert Standard. The Daubert Standard [12] [14] in a way extended the Federal Rule of Evidence and provided clarification to grey areas of Rule 702. The Daubert standard occasioned by Daubert v. Merrell Dow Pharmaceuticals, Inc case provided specific details on the requirements for the admissibility of evidence.

In Daubert, the court agreed on a set of guidelines for scientific admissibility of evidence. The first of these guidelines identifies the court as the gatekeeper, the custodian that ensures scientific testimony accepted by the court proceeds from scientific knowledge or methodology. Scientific methodology incorporates activities such as formulating hypotheses, testing and falsifying hypotheses. This requires that methods claiming to be scientific must embody elements of scientific methodology in hypothesis formulation, testing and falsification of hypothesis. The second guideline required that scientific evidence presented before the court must be relevant to the case and be grounded in scientific principles. As a third guideline, the court in Daubert provided key factors for determining whether the criteria for scientific admissibility are met. The first of these criteria is general acceptance, which tests whether the theory or technique used by the expert is widely accepted in the scientific community. The second criterion tests whether the theory or technique has been subjected to peer review and publication. The third criterion tests whether the theory or technique can be tested and has been tested. The fourth criterion tests whether the technique has an acceptable known or potential error rate. The fifth criterion tests whether standards exist and are maintained which control the theory or technique's operation [12] [14]. The Daubert standard using these guidelines and criteria provides comprehensive tests for evidence admissibility in the courts. The enforcement of the Daubert standard is, however, flexible and dependent on the discretion of the trial judge.

The three standards discussed, the Frye standard, the Federal Rules of Evidence Rule 702 and the Daubert standard continue to play a major role in the United states courts and have influenced standards of evidence admissibility in other parts of the world [2].

## 2.5 The Scientific Method

The scientific methodology follows a general pattern of process cycle from the formulation of a problem to the eventual contribution of new knowledge to the body of knowledge [3]. In the investigation of problems, special methods are often applied. These special methods apply the scientific method within the context of the problem with varying techniques from the general pattern. These special methods can be referred to as paradigms of the scientific method [26] [27].

Paradigms provide a set of ideas and processes which are based on established general patterns and approaches to solving problems. In applying paradigms to scientific inquiry, the general pattern of scientific investigation provides a series of steps in the application of the scientific method [3]. These steps include the problem statement, formulation of hypotheses, derivation of logical inferences based on deductive reasoning, design or specification of test techniques to test hypotheses, evaluation and interpretation of test results and the evaluation of new problems arising from the application of the method. The application of the scientific method is a cycle as it is applied again and again at the end of each cycle as new knowledge and problems are evolved.

In digital forensics, several methods have been proposed with the aim of applying science to digital forensics. These methods are explored in the next chapter of this dissertation.

## 2.6 Summary

This chapter introduced forensic science as a field and discussed a brief overview of forensic science disciplines based on the National Institute of Science and Technology (NIST) current classification of forensic science disciplines are highlighted. Furthermore, the relationship between forensic science and the law and the intricacies that outline this relationship as well as the impact of the forensic science on legal matters are highlighted. The requirements for the legal admissibility of scientific evidence remain a very important aspect of this chapter as it emphasises the role of the scientific method in the admissibility of evidence in the court of law. The scientific method also enables the systematic process of generating and incorporating new knowledge into the scientific body of knowledge.

The next chapter focuses on the methods applied in digital forensics literature that have the specific goal of providing a scientific basis for digital forensics. The chapter explores digital forensics processes and further investigates peer reviewed research in the field of digital forensics with a focus on digital forensic examination methods and how these methods are applied in digital forensics. The forensic examination methods explored include Gladyshev's examination method which observes digital evidence from a finite state level of granularity using a finite state machine, Carrier's examination method which is based on applying a hypothesis-based approach to digital forensic investigations and Cohen's examination method which studies digital evidence from the bit level, a bag of bits. Also, methods proposed by Pollitt as well as Olivier are discussed.

# Chapter 3

# Digital Forensics and the Science of Digital Forensic Examinations

This chapter investigates peer-reviewed research carried out in the field of digital forensics with a focus on the methods geared towards the examination of digital evidence using a scientific approach. These methods are explored by examining the theories from which the methods are derived, the application of the methods, the results that can be obtained from their application and the reliability of findings based on the application of these methods in digital forensic examinations. The goal of this chapter is to provide a background on research done in digital forensic examinations.

## 3.1 Digital Forensics

Digital forensics can be broadly defined as the process that involves the identification, extraction, preservation, and examination of digital evidence and the reconstruction of the events around the occurrence of the evidence under examination. Using this broad definition, digital forensics can be seen to encompass scientific and non-scientific activities during the processes covering the entire investigation.

In observing forensic science disciplines, it can be noted that digital forensics bears the marking of the universal forensics. This is evident in that almost all output from all forensic science disciplines are obtained by using digital equipment and software used in analysing data to obtain the results that can be interpreted by the forensic examiner. These pieces of digital equipment and software and the output of the computational process of these tools are all within the domain of digital forensics [41].

Digital forensics as a maturing forensic science discipline [4] continues to evolve with technology. As information and technological advancement increase, the role of digital forensics and the need to develop tools and processes to cater for investigations and analyses across disparate information cannot be over emphasised. This is prominent as information relates to outputs from computational processes and considered to be artefacts or digital evidence [10].

The alignment of digital forensics with computing is also striking. Digital forensics examines artefacts which are generated by computational processes. An understanding of the computational process underlying a digital system enables an examiner to analyse the operations within the system in a predictable manner. While a piece of software cannot be said to be a 100 percent reliable, the goal of digital forensics is to determine methodically the what, and why of actions that caused the digital evidence that was observed.

This chapter focuses on reviewing methods that have been applied in examining digital evidence. Before delving further, it is important to provide a more formal definition for digital forensics. Below are a few definitions for digital forensics in literature.

What is Digital Forensics? Digital Forensics has been defined in various ways. The following are two notable definitions of digital forensics as defined by Zatyko and at the Digital Forensic Research Workshop (DFRWS). Zatyko in forensic magazine [68] defined digital forensics as: "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability and possible expert presentation."

The DFRWS in 2001 [45] defined the science of digital forensics as "the use of scientifically derived and proven methods towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or/and furthering the reconstruction of events found to be criminal or helping to anticipate unauthorised actions shown to be disruptive to planned operations."

A more general definition of digital forensics refers to the processes, techniques and tools for the identification, extraction, preservation and recovery, examination involving analysis, interpretation, attribution and reconstruction of digital evidence in a forensically sound manner through the application of scientifically proven methods suitable for presentation in the courts of law [4] [61] [38] [5] [30] [10]

What is Digital Evidence? Digital Evidence according to [68] [58] is any information of probative value that is stored or transmitted in digital form.

The probative value of digital evidence is that it is required and sufficient in its ability to prove a case or aspects of a case in court [9]. Digital evidence may comprise of text, numerals, images, sound or video. It may also be in the form of bank statements, spread sheets, emails, and so forth. [59]. Digital evidence can be easily created, altered, forged or destroyed. Digital evidence may also be latent and require the use of special tools or software to extract and make sense of the evidence [11]. It is required as a legal standard that digital forensic tools are validated and properly applied by well-trained professionals. In this dissertation, the reader will come across terms like artefacts, effects, side effects, phenomenon and occurrence. These terms are used to illustrate digital evidence within the context of use. An effect is a direct result of a cause or root cause and side effects are traces which may have been left behind due to the cause. These terms are explained in greater detail in subsequent chapters.

### 3.1.1 The Digital Forensic Investigation Process

In digital forensic examinations, practical activities are usually carried out when investigating digital occurrences or incidents. These activities provide a forensic examiner with a systematic procedure which incorporates scientific approaches. This section discusses the digital forensic investigation processes.

Valjarevic [55] [56] in his digital forensic investigation process model defined five classes of investigation processes. These classes are readiness, initialisation, acquisitive, investigative and concurrent processes. The first class of processes are the readiness processes. These processes occur prior to the start of the digital investigation and are aimed at ensuring the requirements for the investigation are covered. These sub processes include identification, collection, storage and handling of possible evidence sources. This readiness class is considered optional as its application depends on the nature of the investigation.

The second class of processes are the initialisation processes. This class of processes involves incident detection, first response and may cover continuity planning and preparation. The third class of processes are the acquisitive processes. The acquisitive class of processes complement the readiness class of processes and involves evidence identification, transportation and storage. The fourth class of processes are the investigative processes. This class of processes cover the examination of digital evidence, interpretation, attribution as well as reconstruction and presentation and the final closure of the investigation. The fifth class of processes are the concurrent processes which are completed throughout the life cycle of an investigation. These processes cover the tasks involved in maintaining a chain of custody, documentation and preservation of digital evidence through the lifetime of the investigations.

There are also various other models of digital investigation process such as proposed by Cohen [11], Casey [7] [1] [45]. In comparison with the model by Valjarevic [55] [56], these models implicitly define initialisation and concurrent processes as forensic principles in their various models.

In order to provide a comprehensive review of the digital forensic processes as understood in the literature, the rest of this section provides a discussion around Cohen's model for digital forensics [11]. Cohen's [11] digital forensic model covers the following processes which include the identification of digital evidence, digital evidence collection, transportation, storage, evidence analysis, interpretation, attribution, reconstruction, presentation and possible destruction of digital evidence. Within these processes, Cohen classified the digital forensic evidence examination phase to include analysis, interpretation, attribution and reconstruction of digital evidence. While all the processes in a digital investigation are important, the examination processes are very important and constitute the most challenging aspects of a digital evidence investigation.

The first process in Cohen's model is digital evidence identification. The identification of evidence places an important role in a digital investigation as unrecognised evidence cannot be collected and preserved and may cease to exist at the time it is required.

Digital evidence mainly exists as traces with digital systems. Using an example of a digital system executing a malicious software, the execution of the malicious software itself is digital evidence. However, these executions are transient when occurring in a digital system and if not actively observed cease to exist. Transient evidence can only be observed using special tools while the evidence is at play. What is typically left in the digital system are traces of the malicious execution. These are also called indicators of compromise [29]. Other examples of transient evidence include network traffic which must be captured at the time of occurrence otherwise it is lost. Traces on the other hand can be observed after the occurrence. These typically include system logs, registry keys and stored data on digital systems.

In digital evidence collection, it is usually considered good practice to collect as much evidence as possible as one may not know when such evidence may be required. First responders typically consider any digital device as constituting potential digital evidence. A crucial requirement when collecting digital evidence as well as any other forensic evidence is that evidence is acquired in a manner that preserves its integrity. Digital evidence is void and considered inadmissible should its composition change when it is collected. The integrity of digital evidence is usually preserved by using a write block device [34] which prevents any change to the structure of the digital device when digital evidence is imaged for analysis.

Generally, it is common to take forensically sound images of digital media considered as evidence. In some cases, the original media may continue to be used or may be retained during the digital investigation. It is also forensically sound practice to validate images created using cryptographic hashes to demonstrate that the integrity of the imaged evidence remains intact. The collection of evidence may be carried out in different ways depending on the type of evidence and the circumstance. In Live investigations, where systems cannot be turned off abruptly for forensic imaging, obtaining a live copy of the evidence will also serve the purpose of the investigation. Obtaining a memory dump of live system provides considerable data for analysis as much of the evidence relating to the case may reside in memory.

Evidence transportation is the process of transporting digital evidence in a way that will preserve the content of the evidence and ensure preservation of the chain of custody.

It is required that the chain of custody is preserved throughout the period of transportation and while the evidence is secured in an evidence locker. Digital evidence can also be preserved by making exact bit by bit image copies of the original media and validated using cryptographic hashes. It is good practice to keep digital evidence away from magnetic and electro-magnetic sources. The use of anti-static bags [1] is recommended in preserving digital evidence such as CDs, Hard drives, motherboards as these artefacts are typically sensitive to temperature, humidity, physical shock, static electricity and magnetic fields.

Digital evidence storage process entails ensuring that digital evidence is properly maintained in a safe environment throughout the lifetime of the digital investigation. It is important to minimise interaction with the original evidence. Storage must be adequately secure to enforce and assure a proper chain of custody.

The next process of Cohen's digital investigation model is the analysis of digital evidence. This process is also the start of the examination phase of digital forensic examinations. The analysis of digital evidence involves an in-depth examination of the digital evidence to confirm or refute claims made pertaining to the case. While this phase is regarded as the most difficult aspect for forensic analysts, it is also considered the main aspect of forensics where scientific activities are typically performed in a digital investigation. As stated in Locard's exchange principle [7] [45], perpetrators typically always leave traces behind on the crime scene and these traces are essential to understanding what happened in a digital occurrence. In analysing digital evidence, examiners look for specific patterns in traces left behind in digital evidence that confirm certain claims made of the investigation. These patterns form a convincing proof that provide confirmation for the assertions made in the analysis [43].

The next phase of Cohen's digital forensic investigation covers the interpretation of the findings of the analysis process phase. Interpretation of evidence has a certain difficulty attached to it. A finding can be interpreted in various ways and it is plausible that conflicting conclusions may sometimes be made when interpreting the findings of an investigation. In interpreting digital evidence, the forensic examiner must ensure that alternative explanations for a finding are considered to make informed assertions and interpretations grounded on facts about the occurrence of the digital evidence. Further support for the assertions can be obtained from other evidence sources which can be applied in reinforcing the claims made regarding the evidence and its interpretation.

The next phase of Cohen's investigation process is evidence attribution. Attribution of digital evidence is based on the analysis and interpretation of evidence. In attribution, a forensic examiner, based on the interpretation of the evidence, links the evidence to its root cause. The attribution of events to actors is often hard to carry out and needs to be backed by other sources of evidence outside the scope of digital forensics such as DNA, fingerprints. There may also be video or audio recordings which confirm actions taken by the suspects or actors. However, in digital forensics, attribution is made to the digital source of the occurrence. This is typically an IP address, GPS coordinates of the location of a digital device, digital fingerprints identifying the source of a file, or origin of malicious software. The actor who invoked the commands or carried out the actions may, however, remain unknown. The process of attribution leads to a demonstrated reconstruction of the events shown to have occurred in a logical manner.

The next phase in Cohen's digital forensic investigation model is the evidence reconstruction phase. The phase is Cohen's final step in evidence examination. The reconstruction of the events is the step by step demonstration of the events that produced the digital evidence with the aim of validating the claims made about the evidence. This process in digital forensics brings all the work done in examination of evidence together. While it is hardly possible to reconstruct the events of an investigation with a 100 per cent certainty, reconstruction can provide a level of certainty for the digital investigation and based on this level of certainty, the examiner can make definite conclusions on the results of the investigation which assist the court to make conclusive findings on the case.

On conclusion of the examination of digital evidence, the findings are presented before the court. The presentation process involves the transmitting of the result of the digital investigation to the attorneys for their review and the presentation of selected evidence in a legal or administrative proceeding. In presenting evidence, the process applied forms the start of the investigation through which the analysis and final reconstruction of digital evidence is presented before the court. It is noted that the presentation of digital evidence in court is considered an art rather than a science, but it is also important to note that in presenting digital evidence before the court, being the gatekeeper, the investigation must be shown to have applied scientific methodology in its processes. The findings of the investigation must be based on the scientific evidence presented before the court and this evidence must be relevant to the case presented to the court [12] [14].

The final process of Cohen's digital forensic investigation model is the destruction of digital evidence on conclusion of the trial. While this process is not always completed as there may be a requirement to continue to preserve the evidence for another trial, evidence and other information attached to the case may be destroyed or returned to the owner after the completion of the legal matter. This is carried out only by order of the court.

In summary, the process of carrying out a digital forensic investigation must be completed in such a manner to ensure that the method applied is scientific and the principles guiding the handling, preservation and examination of evidence are applied to ensure that the evidence holds up firmly in the court of law. The next section discusses applying scientific methodology specifically in examination of digital evidence.

### 3.1.2 The Science of Digital Forensic Examinations

While digital forensics covers several processes, in this chapter, the focus is mainly on the methods applied in the examination of digital evidence. Digital evidence examination is a complex process which requires that a forensic examiner exhibit an in-depth understanding of the architecture and the underlying technology of the system from which digital evidence is extracted. This includes the various parts of the system such as the mechanism applied by the control logic of the system to determine how the system processes, interprets and displays information. Forensic examiners are also required to have a comprehensive understanding of how to apply the scientific method with the goal of properly interpreting the output from forensic tools which are applied in gathering as much information from the evidence as possible while eliminating flaws in analysis.

The examination of digital evidence involves four main processes. These include evidence analysis, interpretation, reconstruction and attribution [10]. These processes employ the use of the scientific method in operation. Casey [8] notes that the application of the scientific method enables a forensic examiner to reason and reach a logical conclusion about important questions involving who, what, where, when, how and why.

As noted in chapter 2, the scientific method follows a series of steps in its application. These steps include the problem statement, formulation of hypotheses, derivation of logical inferences based on deductive reasoning, design or specification of test techniques to test hypotheses, evaluation and interpretation of test results and the evaluation of new problems arising from the application of the method [3]. The application of the scientific method is a cycle as it is applied again and again at the end of each cycle as new knowledge and problems are evolved.

The scientific method in digital evidence examination begins with the problem definition. This requires the forensic examiner to understand the intricacies of the case to be investigated. While it may not be possible to completely contextualise the case from the very beginning, the examiner is able, based on the knowledge of the system, to determine the facts of the case. Based on the facts, an examiner can proceed to the next stage of the scientific enquiry.

The next stage in the scientific method is the forming of the hypothesis based on the facts and observations made. This is the theory or set of theories that explains the existence of the digital evidence. Hypothesis formulation leads on to experimentation and testing. The aim of experimentation and testing is to determine whether the hypothesis can be strengthened or falsified, and this enables the examiner to determine whether the digital evidence aligns with the hypothesis. This involves reconstructing the events that may have occurred to confirm or refute the hypothesis formulated. Experimentation eventually would lead to falsification or general acceptance. However, there are occasions where the findings are inconclusive. This may occur in situations where there is insufficient evidence available or where there is evidence of tampering. The final stage is the conclusion where the findings and result of a thorough analysis are presented. These findings are presented to the court or other decision makers as proof to a certain degree of certainty [8].

In applying the scientific method to digital forensic examination, several models have been proposed and are currently in use. These models are designed to ensure that scientific methodology is applied in the examination of digital evidence. In the next section, we provide a study of the scientific approach employed in a few digital forensic examination models. These include Gladyshev's examination model, Carrier's model of digital evidence examination and Cohen's model of digital evidence examination amongst others.

## 3.2 Digital Forensic Examination Models

This section is focused on discussions around models that have been applied in the examination of digital evidence in the literature. Several approaches have been proposed with the goal of introducing science to digital forensics when digital evidence is examined. These approaches include methods by Gladyshev, Carrier, Cohen, Pollitt and Olivier amongst others. In this section, the approaches employed by these methods are discussed. The first model discussed is the approach by Gladyshev [20] [18] [19] which explores an approach to examining digital events represented as states in a finite state machine. The second model discussed was proposed by Carrier [5] [6] explores the application of a hypothesis-based approach to digital forensic investigations. The third model discussed was proposed by Cohen [10] and is focused on studying complex occurrences starting from its granular form, a bag of bits from which the forensic examiner proceeds to make sense of the investigation. Furthermore, approaches employed by Pollitt [46] [47] and Olivier [41] [39] are also discussed in this section.

The work by Gladyshev provides one of the notable approaches to establish a scientific basis for digital forensics. Gladyshev's examination model defines an approach to examining digital events represented as states in a finite state machine. Gladyshev's Finite State Machine approach(FSM) [20] [18] [19] [41] [40] can be summarised as an approach to finding all possible paths through a finite state machine, and in essence all possible scenarios of an incident. Gladyshev's model applies an event reconstruction algorithm to compute possible explanations of the incident. The key aspects of the model are the evidential statement and the known facts. The evidential statements are propositions or statements which represent known facts obtained from the evidence. The known facts are truth statements which are accepted as facts of the case. The known facts provide context for the investigation. The known facts also restrict the finite state machine to a limited number of possible computations which enables plausible findings to be made from the investigation.

Gladyshev's approach seeks to demonstrate the application of a finite state machine in formalising event reconstructions in digital investigations. In his work, Gladyshev notes that any program can be mapped to a finite state machine. Gladyshev expressed the representation of a digital system or a program as a finite state machine depicted as a graph. This depiction provides a view of the system to the forensic examiner in two layers; the higher layer being the program and the lower layer being the finite state machine. The finite state machine represented as a graph displays the states and transitions within the system. States are points on the graph while transitions reflect changes in state from one state to the next state. Based on this representation, all possible states and state transitions can be represented and reconstructions from a state can be made by tracing all transitions leading to the state.

In determining the plausible explanations for what may have happened in an incident, Gladyshev notes that knowledge applied by the forensic examiner are in two categories. The first category is the expert knowledge of the system's functionality and design while the second category is the knowledge of the system's final states and outputs from each state in the system. The findings are made from observing a system's state and the transitions between the states in a finite state machine at a point in time that enables a forensic examiner to evaluate and reason about plausible explanations. These findings also enable an examiner to determine whether the hypotheses made cover all aspects of the investigation and to demonstrate a plausible reconstruction of the events that have occurred while also making informed inferences about an investigation.

There are several limitations in Gladyshev's finite state machine method. It is very likely that state explosion will occur due to an exponential increase in the number of states within any given system and especially in complex systems. In addition, while it is possible theoretically to represent the entire set of states in a system, this approach introduces prohibitive costs, time constraints and complexities in computation. Olivier [41] in reference to Gladyshev's model, illustrates these complexities using an example of a system with $n$ bits of storage. $n$ bits of storage in a digital system would have $2^n$ possible states. Where additional storage is added, the states to be represented in the finite state machine grows in exponential proportion and becomes unmanageable and inevitably leads to state explosion. This makes Gladyshev's approach practically limited in its application to real-life scenarios.

Carrier's model [5] [6] explores a hypothesis-based approach to digital forensic investigations. The basis of Carrier's work is to formulate a hypothesis or a set of hypotheses and test these hypotheses to validate or invalidate them. Carrier considers artefacts to be of two main types namely primitive artefacts and complex artefacts. Primitive artefacts are lower level hypotheses which are formulated about the design and capabilities of a system. These are the building blocks and are mainly based on information that can easily be measured or observed within the system. Complex artefacts on the other hand are higher level hypotheses which are derived from observing and testing primitive artefacts. In Carrier's model, complex artefacts are the primary interest of the forensic examiner in an investigation. Complex artefacts are hypotheses made about higher level system events that are investigated by a forensic examiner.

Carrier in his work notes that the development of higher level hypotheses is where an investigation typically starts. While primitive artefacts are of secondary concern to the forensic examiner, they may still be tested for validity to show that the artefacts are valid. However, complex artefacts are typically examined on the assumption that primitive artefacts that constitute their building blocks are valid or can be tested and shown to be falsifiable. Carrier, however, notes that all the claims made about the states and events in a digital system require some degree of testing and these claims may be higher level hypotheses or lower level hypotheses.

In separating lower level hypotheses from higher level hypotheses, Carrier considers artefacts like the time when an event occurred, information on the size of a disk, data file types and system configuration as primitive artefacts. Carrier notes that primitive artefacts may not be completely reliable. For example, Carrier notes that formulating a hypothesis on the time of occurrence of an event cannot be completely relied upon due to the nature of digital evidence. Also, though Carrier's method relies on testing lower level hypothesis, it can be noted that lower level hypothesis is better tested by measurement or observation. The time of occurrence, the size of a disk, the file type and the configuration of a system are measurable and observable artefacts that may not require the use of hypothesis as stated by Carrier [41].

It is much more realistic to calculate the time of occurrence of an event or measure the size of a disk to ascertain a conclusion than to hypothesise about the time frame the event occurred or the size of the disk [41]. Carrier also noted that the theories in most forensic science disciplines are published, generally accepted and testable. However, Olivier [41] noted that Carrier's work leads mainly to contextualised theories and not theories which are published, tested or generally accepted. In a similar effort Olivier [41] concludes that Carrier's effort to apply hypothesis testing where it is more suitable to measure or observe does not make digital forensics more scientific.

Carrier, like Gladyshev, also represents a system as a finite state machine. An important difference between Carrier's characterisation of finite state machine and Gladyshev's is that in Carrier's characterisation, states can change from transition to transition. Carrier also suggests that the finite state machine itself can change between transitions using an example of system changes due to the mounting and unmounting of disks. It can also be noted that both Carrier and Gladyshev design their models in layers. However, Gladyshev focuses on the lower layer, where states and transitions between states in the finite state machine are examined while Carrier focuses on the higher layer, in developing and testing higher level hypotheses or complex primitives. Like Gladyshev, Carrier's model also suffers from state explosion in the finite state machine due to the exponential increase in the number of states as more artefacts are added to the finite state machine.

Carrier's examination process based on the scientific method includes the processes of observation, hypothesis formulation, prediction and testing. In the observation process, the system is observed, and relevant information collected for analysis. The process of hypothesis formulation is based on what is observed. In this process, high-level and low-level hypotheses are formed based on relevant information obtained from observing the system. Based on the hypotheses formulated, the digital forensic examiner can make predictions about the system and test these predictions against the evidence to validate or invalidate a claim.

Cohen [10] in his work explores the physics of digital information as a new science that can be suitable as a scientific background for digital forensics. His research work explores the definition of rules that are accepted as facts within the field of information physics. These facts are then applied based on this science to digital forensic examinations with a view to validate or refute a claim or a formulated hypothesis.

In defining rules within the physics of digital information, Cohen starts by defining the attributes of digital data at the finite granularity of digital information, a bag of bits. Cohen [10] notes that digital information essentially exists in two states. These two states can either be represented as true(1) or false(0) and digital information is capable of transitioning only between either of these two states. Cohen notes that in a digital forensic examination, this level of granularity makes digital information predictable and limits the possibilities when representing information and system instructions to a finite number of values.

Cohen further notes that this same granularity can be observed with digital time which is expressed in clock cycle times and rates or instruction processing speeds and rates. This indicates that in a digital system, there are a limited number of instructions a system can perform at any point in time. The predictability of digital information is further enhanced as time itself is limited and therefore a finite data representation in finite time offers more predictability in a digital system. A system's instruction processing speed and the rate at which instructions can be processed by a system in relation to the time of occurrence can enable a forensic examiner to determine facts about the capabilities of the system and how it would process digital information should this information be required when examining the system or analysing evidential data.

In pursuing the physics of digital information, Cohen observes the nature of digital data in relation to physical mechanisms and how observation affects their states. Cohen notes that digital data can be observed without altering its state. While physical mechanisms that represent the data may be altered slightly when the data is observed, these changes are not large enough to change the state of the bits represented. Aside from observation, exact replication of data can be achieved without altering the original state or content of the original data. This poses several problems for a digital forensic examiner. Information can be copied without affecting the validity of the original information, and information can be transferred from one source to a destination without affecting the source of the information. This indicates that information can also be created, altered and stolen without it being noticed.

In order to make sense of digital information, there is a need for the information to be provided within a contextual frame. Cohen noted in his work that the result of an examination can only have value when interpreted within the context of the occurrence. Cohen limited the context of digital information to be within the FSM through which the information is processed and the interpretation of digital information to the resulting states and output observed or traces within the FSM.

Cohen observed that FSMs have many properties; one unique property is that due to incomplete traces seen in FSMs, knowing the current or final state and the finite state machine means that an examiner will be able to determine what prior states occurred, the inputs and the sequence through which the final state was reached. However, as finite state machines may have transitions from an initial state through a sequence of states and reach a final state which may be identical to the state from which the finite state machine initially started, the examiner may find that initial states and inputs in those states may not be unique. This implies that the current state of the FSM does not imply that its history or initial states are unique and that an effect or trace observed may have different plausible causes. While Cohen's focus initially was on finite state machines, Cohen notes that a Turing machine is achieved with the addition of an unlimited tape to a finite state machine.

Cohen then goes on to discuss the limitations of finite state machines and notes the role of computational complexity in examining digital information. Cohen [10] notes that where the mechanism of a finite state machine is clearly understood, the transformation of digital nodes in a finite state machine from one state to the next requires space and time which is proportional to the mathematical properties of the transformation. This implies that the input, state and configuration of a finite state machine determines the number of steps to achieve a desirable output. Additional input at a certain state in a finite state machine may influence the time required to reach the desired output.

The focus in Cohen's model is mainly on understanding the nature and structure of data and how this structure can be applied in examining digital evidence. Cohen also examined higher level structures i.e. programs in operating systems and notes the impact different versions of programs have on evidence examination providing additional structures that produce effects or traces within the system. The knowledgeable examiner would be able to contextualise the information obtained based on the differences each program version introduced to the system.

In much of Cohen's work, the overarching theme is to determine all the factors and constraints that can be observed in the identification, analysis, interpretation, attribution and reconstruction of digital evidence and the limitations that are often observed in the validity and consistency of results that can be obtained from a digital evidence examination. Cohen's work relies heavily on the physics of digital information with the basis that it provides the underlying information required for a forensic examiner to properly identify, analyse and interpret evidence in a clear, concise way.

Cohen built on the background provided in his work on information physics and further explored issues relating to the design and reliability of digital systems as well as the reliability of forensic software used to examine and analyse digital information. Cohen also explored and defined processes that are part of the digital forensic evidence examination starting from evidence analysis and proceeding to interpretation, attribution and reconstruction of digital evidence.

An alternative approach that moves away from formal computational models applied by the previous three models discussed is one that applies two literary theories, narrative theory and surrealism from the field of humanities and was explored by Pollitt [47] [46]. Pollitt in his work applies the theory of the narrative to derive a context and "story" or explanation for the evidence under examination and the theory of surrealism to derive a meaning from the evidence.

Pollitt [46] before introducing the ideas around his theories, makes a series of assumptions about digital information and digital evidence. Pollitt notes that in general, though evidence can be massive in size, most of what is relevant in a digital investigation for probative and exculpatory purposes is a small subset of the original evidence collected from the scene of the crime. In addition, Pollitt hypothesised about the digital space, the continued growth in the size of storage media, the increasing application of computing devices, the continued increase in the amount of private and personal information residing in electronic storage and how much information about an individual may be obtained from these devices. These hypotheses continue to hold true as technology continues to proliferate and find new areas of application.

Pollitt starts his examination by exploring the concepts of digital data, digital artefacts and digital media. He observed that digital data can be defined as "text" that is contextualised and has a meaning. According to Pollitt, "text" is not merely a number, letter, words, sentences or even paragraphs, but is a recording that is meaningful within a certain context. Digital artefacts or digital evidence such as program files, web server logs and network activity logs are considered as text and the digital media that stores these texts represent the collection, an anthology store or a digital anthology.

Pollitt applies two main theories in his work, the theory of the narrative and the theory of surrealism. In applying the narrative theory, Pollitt defines a narrative as a "story" that describes the text. The theory of surrealism on the other hand is applied to derive meaning from the text. Pollitt noted that the adherents of surrealism applied the theory mainly in games where the purpose of the games was to suppress the individual's consciousness and allow the unconscious to fuel the individual's creativity. The idea behind applying surrealism to digital examinations is to disrupt the flow of the narrative by integrating the use of montage as a technique. Montage is applied as a technique that observes a part of a whole in isolation. The strategy is then to place the parts together to form a narrative, a plausible explanation for the evidence. Pollitt defines what he termed the surreal narrative in which the narrative context and the montage are applied from surrealist games to digital forensics.

Pollitt notes that in examining an individual's anthology, an examiner seeks to identify all the data points that are relevant to a specific theme. Where the theme is that of a digital crime investigation, an examiner identifies data points that indicate suspicious criminal activities within the individual anthology. Much of the criminal plot in a digital crime will be recorded in electronic media, an examiner is able to examine data points in the media which provide a valuable amount of data points to the "subplot" of criminal activity. Pollitt notes that the problem mainly encountered by an examiner is not a lack of data and context, it is that a person's life consists of various different complex data points that are written in different contexts and limiting these data and contexts to a manageable amount that provides an accurate picture of the individual in the context of the "subplot" can be a challenge for the examiner. Digital forensics according to Pollitt is made up of several nested narratives which include the narrative of how the digital evidence came to be and the narrative of the content of the digital evidence. The problem encountered by examiners is to identify narratives from the evidence and demonstrate a coherent complete meta-narrative from the selected narratives.

Pollitt noted that to build a system that applies the core concepts of the narrative and montage, three things are mainly required. The first is to parse the electronic media or digital evidence into narratives, the second requirement is to formalise the narratives and the context of the investigation in a formal language or code for it to be computable. The third requirement is to understand the different levels of completeness and reliability of the narratives to apply appropriate weights for making reliable inferences about the examination.

A final approach discussed in this chapter that seeks to apply science to digital forensics is Olivier's work on algorithmics [39]. Olivier in his research proposed algorithmics as a suitable foundation for digital forensic science. The focus of his work was on applying probabilistic algorithms to a whole range of problems that are considered intractable or "hard problems" in computing. Olivier's work is significant as it applies this method to a difficult part of forensic science that several methods have been unable to satisfy, the determination of the rate of error of computations. Olivier notes that a forensic examiner can answer questions about the error rate accurately if the problem faced is probabilistic in nature. Olivier, however, noted that theoretical results are often obtained from tools and applications and the implementation of these tools is not without error. Error in tool implementation introduces error rates in forensic tests and these error rates are dependent on the input as certain tests produce different error rates when applied in different situations.

## 3.3 Summary

In this chapter, the science of digital forensics has been discussed with the main aim of demonstrating how science has been applied in digital forensic examinations. While this chapter has focused mainly on discussing models proposed by Gladyshev, Carrier and Cohen, there are other models in literature that are relevant to the science of digital forensics. These models have also sought to achieve the same purpose of proposing a scientific basis for digital forensics. They include Casey's model for digital forensic investigation [8], Pollitt's model which applies narrative theory in digital forensic examinations [46] and Olivier's work on the application of algorithmics in digital forensic examinations [39]. These research works contribute extensively to the body of knowledge of digital forensic science. It is important to note that this dissertation complements the work done by these authors in achieving a scientific basis for digital forensics.

The next chapter introduces case study research as a method for digital forensic examination providing detailed discussion on various aspects of the method. The chapter explores case study research as a scientific basis for digital forensics. Furthermore, Virchow's autopsy method is examined as a specialised approach of case study research focused on performing post-mortem examinations in the medico-legal profession. While case study research is seen in this chapter as a generalised approach to forensic examinations, it is shown to be suitable for specialised applications in digital forensic examinations.

# Chapter 4

# Methods in Science and Forensic Science as Paradigms for DFE

How do we examine forensic evidence? How do we make decisions or inferences about what we have examined? How do we validate these inferences to show that our claims are justified, and we are not biased in our conclusions? These questions are asked by a forensic examiner every time an examination is required. There are, however, other equally important questions that a digital examiner may fail to consider which are crucial to ensuring that the examination is a valid one. These questions look at the "scientificness" of the method used in examining the evidence. The Daubert standard [12] [14] states a number of these questions and provides criteria for ascertaining the "scientificness" of a method. A discussion on the Daubert standard was provided in chapter 2.

The field of digital forensics has made considerable progress in research [42] but is yet to attain a level of consistency and certainty comparable to those obtained in DNA analysis mainly in inferences made during examination of evidence [36].

The highest state of inference in a digital examination is determining causality. Causality relates to cause and effect. It is the determination of attributable causes in relation to specific incidents, events or actions [62]. Inferences in a digital inquiry are made mainly during evidence examination.

For evidence to be considered admissible in the court of law, a prerequisite is for it to be obtained through a forensically sound approach. A forensically sound approach indicates that the principles and practices involved in the determination of the findings obtained from the evidence and the conclusions inferred from the findings are grounded in science [36].

To ensure the findings are grounded in science, a forensic examiner may apply a general approach such as a scientific method or a specialised method established within a scientific discipline or field of study such as forensic science. The scientific method is the body of knowledge which is tried and tested from which scientific principles and practices are derived and applied in the examination of phenomena, the acquisition of new knowledge and the validation of already accepted knowledge [3] [27]. A specialised method such as used in a forensic science field is also grounded in scientific method. However, it provides an inquiry based on definitive processes and patterns of reasoning for extracting and analysing information when examining specific events without tampering with the evidence in a way that jeopardises the entire investigation.

Therefore, in establishing the cause and effect findings during evidence examination, a forensic examiner must be able to show that scientific principles and practices grounded by a scientific method or a specialised method in the forensic science discipline (grounded in a scientific method) was applied, the outcome of which demonstrates the reliability of the processes employed in evidence examination and ultimately the findings of the examination phase.

The use of methods in science and forensic science as paradigms for establishing cause and effect (causality) is well documented [27]. A paradigm is a framework that brings together accepted concepts, theories and ideas which provide direction on how research should be performed [27]. The application of methods in science and forensic science as paradigms provide a consistent and reliable approach to ensure the legitimacy of the findings of an inquiry. This is one of the main goals of the research, to consistently apply methods in science and forensic science as paradigms in the determination of cause and effect in digital forensics.

In the natural sciences, two methods that may be applied to digital forensics to determine causality are experimental research and case study research [65]. The use of experiments is well tested and scientifically accepted as a method for determining causality [6] [3] [16]. The case study research method, while also an accepted scientific method is not widely used in the natural sciences [65]. Although experimentation is used for a whole range of scientific studies, there are situations where it is not always possible to carry out an experiment. In these cases, the only option left would be to carry out a case study. In other cases, though experimentation is possible, carrying out a case study may reveal even more findings during the examination phase than an experiment can provide.

In the field of forensic science, and within established forensic science disciplines with well-defined methods, there are methods that can be applied as paradigms in digital forensics. One of these methods is Virchow's method of autopsy. Virchow's autopsy method is a specialised forensic science method of carrying out an examination to determine the cause of death in a forensic environment. Virchow's method was the first systematic method developed for autopsy and has become the standard method for performing autopsies.

This chapter introduces the application of the case study method, a general method of scientific inquiry and Virchow's autopsy method, a specialised forensic science method as paradigms for digital forensics.

## 4.1 The Case Study Method as a Paradigm

To provide a clear perspective in this section, a definition of terms is provided.

A case is an instance, an event, an occurrence or a phenomenon. A case for example may be a police investigation of illegal drug use, a criminal or civil proceeding where the court makes a finding that reflects "the truth" based on the expert witness testimony and evidence before it, a "network breach" case where the intrusion is investigated to determine the cause and the actors. Investigating a case is essentially carrying out a "case study". In a forensic context, a case study would likely start at the examination phase of an investigation. The investigation, however, may also form a larger case study. However, the focus of this research on the examination of evidence restricts the scope of the case study to the examination phase of the investigation, typically to what would be carried out in the laboratory.

As shown above, the term “case” has a different meaning in legal and scientific settings. To avoid ambiguity, the use of the word “case” will not refer to a legal case in any sense but will always refer to the instance, event or phenomenon of interest observed in the case study. When referring to a legal “case”, we use the word “proceedings” as in legal proceedings.

In the sciences, a case study may be a descriptive, an exploratory or an explanatory analysis of a case. A descriptive case study aims to illustrate an event and the exact context of the event. An exploratory case study aims to define the research questions and hypothesis pertaining to an event. An explanatory case study aims to establish causality.

Yin [65] defined a case study as two-fold: 1) the scope and 2) the features of the case study [65]. In terms of the scope, a case study is an in-depth investigation of a real event the cause of which is not fully understood and is investigated taking into consideration all the conditions or circumstances that formed the event. In terms of the features, a case study copes with events exhibiting complex conditions, relies on multiple sources of evidence and supports the notion of theoretical proposition [65].

The above definition highlights why a case study is relevant. A case study helps an investigator to understand a phenomenon while considering all the conditions pertaining to the phenomenon. This differentiates a case study from an experiment which typically occurs in a “controlled” environment. Therefore, an experiment cannot cope with events exhibiting complex conditions [65].

According to Yin, a case study, like an experiment, can be used to answer “how” and “why” questions [65]. Yin also noted that “the more your questions seek to explain some present circumstance (e.g., “how” and “why” some social phenomenon works), the more case study research will be relevant”. Answering “how” and “why” questions is an approach to establishing causality. This is essentially determining the root cause of an event, a process called root-cause analysis [21]. Note that the word “social” phenomenon is used. Yin’s approach to case studies is designed from a social science perspective. However, Yin did say that “. . . case study research is commonly found in both the social science disciplines and the practising professions” [65]. Digital forensics is a practising profession therefore an applicable field for case study research.

## 4.2 Case Study Design

The design of a case study can be considered as having two main aspects that are relevant. The first aspect incorporates five design components necessary to carry out a case study. These are the questions of the case study, the hypotheses of the case study, defining the unit of analysis, linking data or evidence to the study hypotheses and finally, specifying criteria for interpreting the findings of the case study. The five design components enable an examiner to approach an examination or case study from a perspective that is based on a logical design. The second aspect of the design of a case study involves the validation of the case study design. This aspect tests the validity of each aspect of the five design components by incorporating four validation tests that assess the quality of the case study design and the findings of the case study. The four validation tests are construct validity, internal validity, external validity and reliability. The rest of this section discusses these two aspects of the Case Study Design.

### 4.2.1 Case Study Design Components

Yin's case study method highlights five design components. The first three components within a case study design are the case study questions, the case study hypotheses, and the unit of analysis. These three components aim at providing direction or focus for the study, assisting the examiner in determining what other evidence is relevant to the investigation and whence such evidence can be extracted. It is important to note that these three design components are carried out before the evidence is examined. The last two components within the case study method are linking data to propositions and the criteria for interpreting the case study findings. Each of these components are discussed below.

**I. The Case Study Questions**

An examination using the case study approach starts with the questions that are asked of the evidence [65] [44]. These questions are what the examiner is expected to provide answers to while examining the case. The questions are usually provided by the prosecutor or the defence. A forensic examiner interprets the legal question (for instance, Did A kill B?) into questions that science can answer (for instance, what fingerprints or DNA type are present at the crime scene or on the murder weapon? Is the genetic type consistent with A's profile?). Answers to these scientific questions can then be used to make inferences and assist the court in answering the legal question [24]. In constructing a scientific question, the element of guilt is lost and all that remains is a scientific question.

Case studies are designed to answer "how" and "why" questions. It may be important to note that to answer how and why questions, "what" questions may also be asked. However, "what" implies identification, a process usually performed before the case study is initiated. While it is likely that "what" questions may come up during the case study, these questions can also be answered during the case study.

### II. Developing the Case Study Hypotheses

These constitute the theoretical propositions or hypotheses that focus the study on what needs to be tested within the study. Hypothesis generation, an integral part of the scientific method [65] [3], is fundamental to any scientific activity. Without the formulation and testing of hypothesis, a scientist cannot confidently state that a scientific activity has been carried out [54] [24] [6]. Hypotheses are formulated by a forensic examiner based on the questions that need to be answered. It also provides clarification on what evidence may be useful and where potential evidence or data may be found. Exploratory studies typically do not have propositions, but rather have a study purpose. Once the questions are known, the examiner formulates a hypothesis or a set of hypotheses or theoretical propositions around the questions [54]. This necessitates the experience and scientific knowledge of the examiner as well as an understanding of the context of the case [24]. The hypotheses establish what the examiner expects to demonstrate about the evidence in question.

In the field of statistics, the development of theories produces two competing hypotheses, the null hypothesis which states that the theory does not hold and the alternative hypothesis which states that the theory holds. Hypothesis testing proceeds by finding evidence that rejects the null hypothesis in favour of the alternative hypothesis. However, in Yin's approach to case study research, various strategies and techniques are applied to derive an explanation for observed facts. These explanations are subjected to testing before they are deemed proper explanations. Colloquially, one may refer to these explanations as hypotheses but in order to avoid confusion with other uses of the word "hypothesis", we will refer to such use of the word as the "main hypothesis". To test the main hypothesis, one attempts to find rival explanations that would also explain the observed facts. Effectively, these are attempts to disprove the main hypothesis. In this dissertation, we will refer to these rival explanations as rival hypotheses when they are tested.

Hypotheses are typically developed in sets with one of them being the main hypothesis and the other, the rival hypothesis. The main hypothesis reflects what the examiner expects to observe and demonstrate within the context of the examination. Rival hypotheses are plausible explanations that oppose the main hypothesis and are required to be disproved. While there will always be plausible rival hypotheses, possibly the defence or prosecutor's version of events, the examiner must gather enough data that would likely demonstrate support for the main hypothesis and/or refutation of the plausible rival hypothesis under study. The examiner's task is to show that given the context of the case, the evidence shows that the main hypothesis is true. The forensic examiner, however, has a duty as a scientist to be objective in the examination of evidence and present explanations which might not benefit his client in the same manner accorded to the main explanations of the case [24].

### III. The Unit of Analysis

This involves the determination of what will be examined i.e. the case based on the study hypothesis as well as the selection of two design choices. The first choice is between applying a single and a multiple case design while the second choice is between a holistic and an embedded design. A descriptive, exploratory or explanatory case study can be designed as a single-case design or a multiple-case design.

A single case design examines a case in-depth to demonstrate whether the hypothesis made about the case is true or that there are rival explanations that can explain the case more explicitly. Essentially, a single-case study is carried out to confirm a hypothesis or theoretical proposition. The goal may also be to capture relevant information or find rival explanations relating to the studied case. According to Yin, there are five main justifications for carrying out a single case study: 1) *A Critical case:* A case where a theory or theoretical propositions believed to be true are studied to determine whether the propositions are correct or whether there are rival explanations which are more valid. 2) *An Extreme or Unusual case:* A case where the event differs from widely accepted theories or normal events. 3) *The Common case:* A case where a normal event is investigated to capture expected conditions. 4) *The Revelatory case:* A case where an event that was previously inaccessible becomes observable. A description of this event alone is revelatory. 5) *A Longitudinal case:* A case where the interest of the research is to determine whether in an event, certain conditions change over time.

A multiple case design examines two or more events to draw similarities and find support for the study findings and/or refute rival explanations by predicting opposing results to invalidate them. When a study requires an in-depth analysis of more than one occurrence or event, a multiple case study is required. A multiple-case study also provides more compelling evidence to support the inferences and conclusions made in the study. Yin noted that to use a multiple case study design, one would have to apply the logic of replication [65]. Yin highlights two sides of this logic: literal replication and theoretical replication. Literal replication aims to predict similar results. A multiple case study with two to three cases would refer to literal replication. The idea is to study a case in-depth and find similar support for the study findings from examining a second or third case to show a web of consistency. The aim of theoretical replication is to predict opposing results and invalidate them. Theoretical replication extends the logic of literal replication. To achieve theoretical replication, an investigator must first achieve literal replication i.e. show that the main hypothesis of the study is supported in multiple cases, two to three cases. After literal replication is achieved, an investigator is required to carry out a further in-depth study of two or three more cases making the disproving of plausible rival hypotheses the goal of the study. In this way, the examiner can demonstrate that the rival explanations cannot possibly be true and, in the process, further reinforce the initial findings of the study.

The secondary design choice is between a holistic design and an embedded design. Here, the aim is to structure the case in such a way that facilitates the ease of study and reduces the complexity of the case when required. A holistic design allows an investigator to study a case in its entirety, while an embedded design allows an investigator to study separately a subunit or subunits of a case. The choice between a holistic and an embedded design depends on the scope of the case. A simple case requiring an in-depth analysis of an isolated event is suitably studied as a holistic case while a complex case with a chain of events will usually require an embedded design. A single case or multiple case design may, however, have a holistic or embedded design.

An example of a unit of analysis may be an entire computer, a local area network, a cloud resource, in the case of network investigations, the units of analysis could span across the Internet depending on the incident. Non-complex cases are simply studied as a single-case study (one case) with a holistic approach which enables the examiner to analyse the incident in depth. The more disperse the likely sources of evidence, the more complex the evidence analysis will be. Complex cases involving disperse events and evidence can be suitably analysed as a single-case study or multiple-case study (two or more cases) with an embedded design. An embedded design allows an examiner to break up a case into subunits that can be examined individually but with a focus on triangulation of events, that is, linking results and findings from each subunit within the one case for single cases, or subunits of each case within multiple cases together to show certain consistencies within the case(s) and ultimately demonstrate a web of consistency that reflects the findings of the examinations.

This is well illustrated in cases spanning several technological platforms and geographical jurisdictions where findings from each jurisdiction are linked to findings from other jurisdictions to test the study hypotheses and to reflect the full context of the case and demonstrate a web of consistency in the conclusions made about the case. At this stage the examiner can identify other likely sources of evidence and where evidence which may need to be examined can be found. The forensic examiner by establishing what evidence is relevant to the examination eliminates the need for mining all evidence for possible hits and allows the analysis to focus on evidence that is immediately useful for analysis.

### IV. Linking Data to Study Propositions

This aspect focuses on testing the study hypothesis and demonstrating consistency and possibly causality in the evidence under analysis. There are two processes within this phase that must be achieved when analysing a case: the selection of a general analytical strategy for examining the evidence and the application of analytical techniques to analyse, interpret and draw inferences from the evidence under study. While the early stages of the case study focus the analysis on immediately relevant evidence, the examiner must now determine what analytical strategy to employ in evidence analysis with the aim of linking evidential data to the hypothesis. This requires strong analytical thinking ability on the part of the examiner and the experience and ability to use forensic tools. While forensic tools are useful in extracting and manipulating data, it remains the job of the examiner to establish useful patterns and triangulations from the data obtained to demonstrate the hypothesis to be tested. In the selection of a strategy, an examiner may choose to come up with an analytical strategy of choice [11].

In the selection of a general analytical strategy, the case study method provides four strategies that an examiner may consider when examining evidence. The first analytical strategy is to rely on theoretical propositions. This strategy focuses on proving or disproving the study hypotheses, an obvious strategy since the questions that need to be answered are reflected by the hypotheses or propositions made about the evidence. The second analytical strategy is to work your data from the ground up. It focuses on the data or evidence, an inductive approach unlike in the first strategy where the focus is on the hypotheses. In applying the second strategy, the examiner looks through the data to find interesting traces or clues that can lead to further analysis. These traces provide a path or paths through which the data can be examined.

The third analytical strategy is to develop a case description. This strategy employs the use of a descriptive framework, or a narrative [46]. A narrative is really a detailed description or story about the event under examination. By applying this strategy, an examiner is trying to tell a story about the occurrence and to provide a context to the case. Developing a case description also allows an examiner to identify explanations that should be analysed.

The fourth analytic strategy is to examine plausible rival explanations. While the above three strategies are extremely useful, there are usually always rival explanations for an occurrence. In some cases, these rivals may not be mutually exclusive. This strategy requires the examiner to identify plausible rival explanations that need to be addressed. This strategy can be applied alongside the other three analytic strategies. For instance, an examiner's initial theoretical proposition may include rival propositions. There may also be other clues found while studying the evidence that lead to rival propositions. The description of a case may also produce rival propositions that should be analysed. By addressing rival explanations, the examiner can strengthen the study findings. These four strategies enable an examiner to link the evidence to the study propositions.

Within each analytical strategy, analytical techniques can be applied. The selection of an analytical technique or a combination depends on the case. Applying analytical techniques is also intended to deal with the problems associated with the requirement for satisfying the validity of a case study which will be discussed in the section 4.2.2. The analytical techniques are pattern matching, explanation building, time-series analysis and logic models and are discussed below. These analytical techniques provide the examiner with an ability to show logically how the conclusions of the examination were made and taking into consideration all the factors that may have influenced the existence of the phenomenon under study.

*Pattern matching* is applied mainly under the first strategy (to rely on the hypotheses of the study) and is a technique applied by comparing patterns based on the findings of the study with the predicted pattern or hypothesis made before the evidence was observed and analysed. For example, an examiner may hypothesise that an individual accessed a certain website and downloaded malicious software that was used to carry out criminal activities and may have deleted traces of the individual's activities. Usually, one would expect to find traces of web activity on the suspect system but if these traces have been deleted on the suspect system, we expect to find a gap in the web browser logs when no web activity was recorded even though the suspect was active online at the time. On accessing other sources of evidence such as web server logs, ISP logs, firewall logs, an examiner may find web artefacts not present (deleted) from the suspect's computer confirming the initial hypothesis that the individual accessed and downloaded the said malicious software. The matching of these patterns, the predicted pattern to the empirical pattern provides a strong argument for the findings made.

*Explanation building* is applied mainly under the second analytical strategy (working your data from the ground up). The whole idea of this technique is to develop a narrative that explains the phenomenon under examination by showing how each piece of the puzzle came to be, the causal links, what caused what to exist and how each piece fits into the whole. It can also be described as an attempt at tracing the interactions of each piece and building up a narrative that explains its interaction with the whole.

*Time-series analysis* is an analytical technique applied in tracing the changes in the state of a phenomenon over time. For example, reconstructing the state of a system at the time a file was created and observing the intermediate states as changes were made to the file until arriving at the final state. Another example is the reconstruction of the web activities of an individual in time. Time-series analysis is therefore a form of reconstruction that aims to specify "how" and "why" a phenomenon came to be.

*Logic model* is a form of pattern matching and is applied to break down complex events into repeated cause and effect patterns to reflect how the conclusions were reached from intermediate findings. This is also a form of event reconstruction. By reconstructing the sequence of events that caused an evidence or phenomenon, a forensic examiner can demonstrate that all the pieces of the puzzle are accounted for.

The use of any of these four analytical techniques within a suitable analytical strategy enables the examiner to demonstrate the findings of the study from the evidence and establish the consistency of the main hypothesis and/or the inconsistency of the plausible rival hypothesis with the evidence.

### V. Findings Interpretation Criteria

Finally, a forensic examiner will have to interpret the findings of the analysis of the evidence using certain criteria [65]. During the interpretation of the evidence obtained from the analysis of the findings, an examiner may identify explanations that rival the findings made from the examination. Addressing these rival explanations can be used as criterion for interpreting the findings of the examination. The more rival explanations are addressed and excluded, the stronger the findings of the case study.

### 4.2.2 Validating the Case Study Design

The validation of a case study design is an important step in demonstrating that the findings made from the case study is consistent and reliable. Yin provides four tests that can be used in validating a case study design. They include tests for construct validity, internal validity, external validity and reliability. In satisfying these tests, important principles or tactics must have been implemented while carrying out the case study. These tests also ensure that the case study is consistent in its claims that the findings of the case study are valid and that these findings are the outcome of a computational process, a process based on an accepted scientific method.

#### I. Construct Validity

The test for construct validity critiques the justification for the evidence collected for examination. It determines whether the data collected is sufficient to answer the questions that are asked of the evidence and tests the rationale behind the examiner's decision on what evidence to collect. What this means in a case study is that the data obtained for the study should be justifiable. Given any question, the examiner must be convinced that the appropriate piece of data was selected for the study.

Three tactics or actionable principles [65] can be applied to strengthen construct validity: the use of multiple sources of evidence [8], establishing a chain of evidence [8] [10] and peer reviewing the study's findings.

The first tactic is to ensure the use of *multiple sources of evidence*. This is consistent with Casey's certainty scale which points out that evidence that is supported in multiple independent sites has a higher certainty value than information on a single source that could have been tampered with [8]. This ensures the case study findings are strengthened by a web of consistency that can be established during the evidence examination. The second tactic is to establish a chain of evidence, an important principle already established in digital forensics [8] [11] [10] [60]. A well-documented chain of evidence confirms that the evidence was handled correctly throughout the lifetime of the investigation. The third tactic is to ensure that the draft findings of the case study should be reviewed by key informants. This is to enable the key sources to validate the information they have provided. In digital forensics, there are no key informants, because the evidence is primarily bits and bytes extracted from a computer system. Therefore, the closest to a key informant review is a peer review of the findings by another forensic examiner or a peer group. This includes a critical discussion of what has been analysed. [44]. This is a new element in digital forensics that is not currently in use. Two subtypes of validity that make up construct validity are convergent and discriminant validity. Convergent validity measures the degree of similarity between data collected and discriminant validity tests the unrelated of data collected for the study. This enables an examiner to assess the accuracy of the study construct relates back to the study data.

### II. Internal Validity

The test for internal validity critiques the findings of a study and is a main concern for explanatory case studies (case studies which apply case description as an analytical strategy.). Internal validity tests the logic that led to the findings of the study to confirm that the findings reflect what was analysed. It critiques the forensic examiner's findings and asks the question "how can be we sure that our findings reflect the outcome of the case and that there are no other factors that may have influenced our findings?" What this means in any case study is that the conclusions should follow from the observation. For example, if an event $E_1$ can cause $E_3$ and an event $E_2$ can also cause $E_3$, how can we explain with certainty that event $E_1$ and event $E_2$ both caused $E_3$ or that even though event $E_2$ was present, it did not contribute to $E_3$.

Four tactics can be applied in strengthening internal validity. These are pattern matching, explanation building, addressing rival explanations and logic models.

The first analytical tactic is *pattern matching.* Pattern matching [65] is a technique that is applied by comparing patterns based on the findings of the empirical case study with the predicted pattern(s) or hypothesis made before evidence collection. The whole idea behind hypothesising is to show that the matching of predictions made before empirical observation provide a stronger argument for the validity of the study. A simple example is if we know a certain web browser was used to access a website, the critical element of a web browser communication is that we expect to find information such as the sender details in the destination web-server log, what browser was used, and the IP address of originating network. Finding these artefacts shows that we are following a structured approach.

The second tactic is *explanation building*, considered a special type of pattern matching. The process of explanation building is mainly to analyse the evidence by building an explanation about the case. Explaining a case is essentially establishing the relationships between the variables or conditions of the case. This is an attempt at interpreting the evidence by accounting for all the conditions that produced the evidence and showing that all the pieces fit into the case.

The third tactic used to meet internal validity is to *address rival explanations*. Rival explanations or theoretical propositions must be developed and expressed in a way that the conditions of these rival explanations are mutually exclusive, that is, if one explanation is valid, the other cannot be valid. For instance, a forensic examiner might recognise a rival explanation for an occurrence, say in a child pornography investigation, where the suspect may claim that a Trojan was responsible. The forensic examiners' task is to rule out the possibility of the presence of a Trojan. Using pattern matching, the forensic examiner can show that for a Trojan to be present, it is expected that certain specific system files would have changed, and certain unusual activities will be present in the system. Proving that these expected changes and activities are not present addresses the Trojan issue and strengthens the findings of the investigation.

The fourth tactic is the use of *logic models* as an analytic technique for internal validity. Logic models are another form of pattern matching. However, it can be distinguished from pattern matching in that it breaks down a complex chain of events into repeated cause-effect patterns to reflect intermediate findings and final findings [65]. This is a form of event reconstruction. By reconstructing the sequence of events that caused the evidence, a forensic examiner can show that there are no missing pieces in the puzzle and account for all the conditions that produced the evidence.

### III. External Validity

The test for external validity tests the generalisability of the study findings beyond the immediate study. It asks the question "will the findings be the same for a similar case". In a case where the findings are causal, the question may be whether or not "for all cases, an event $E_1$ will always cause another event $E_2$?". To fulfil this requirement, an examiner may consider applying analytical generalisation which aims to show that the findings of a case explain what was observed in that specific case. However, if in another similar case, an examiner finds that there may exist another possible explanation, then it is important to show that the findings of the previous case do not apply. The tactics applied in strengthening internal validity are also applied to strengthen external validity.

**IV. Reliability**

The reliability of a case study is crucial to ensuring that its findings are consistent, and a structured approach was followed in carrying out a case study. The goal of reliability is to minimise errors and bias in a case study. To ensure reliability, the case study must provide a full documentation of evidence, processes as well as the actions taken throughout the study. The importance of documentation is to show that a structured approach was followed in carrying out the case study and if the same case study were to be repeated by another examiner using the same procedure, it would be very likely that the other examiner would arrive at the same conclusions.

In summary, these four tests (construct validity, internal validity, external validity and reliability) can be applied in assessing the quality of case study designs. These tests ensure that the study findings are consistent with the underlying theoretical propositions, have been peer reviewed, and that the case study is repeatable and rival explanations are taken into consideration to reinforce the study findings.

### 4.2.3 Modelling the Case Study Design

Figure 4.1 and Figure 4.2 displays design model of the case study. In Figure 4.1, The model is illustrated as from a bird's eye view while Figure 4.2 is a detailed model incorporating the design components, validity tests, principles or tactics as well as the strategies and techniques for carrying out a case study in a logical manner. These models are not discussed again in this section as they have been discussed in earlier sections of this chapter.

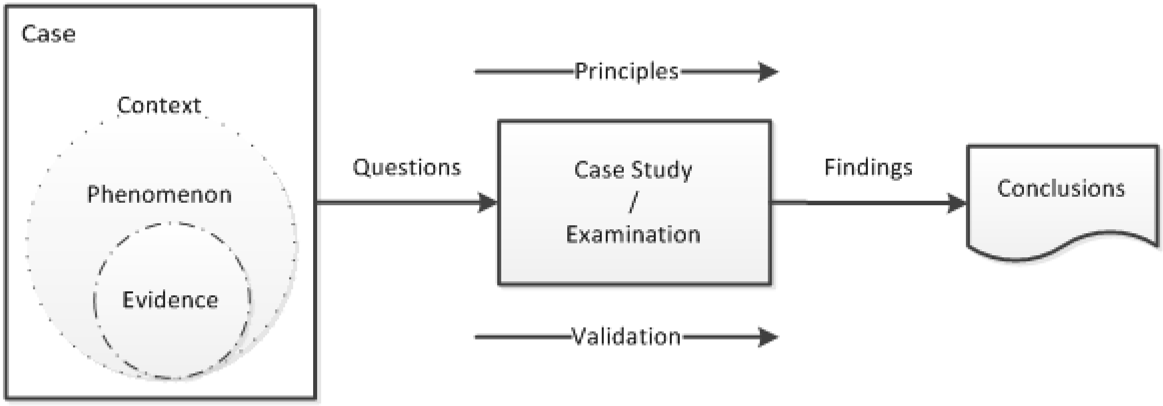


**Figure 4.1:** A Model of the Case Study Design.

### 4.2.4 Examples on applying Case Studies in digital examinations

In digital forensic investigations, the examination of digital evidence starts when the first responder hands over forensically sound copies of the digital evidence and a case file to the forensic examiner. The case file contains details of the "case" and the questions that need to be answered by the examiner. The goal of the forensic examiner is to demonstrate his findings based on the evidence. We examine three basic case study examples below.

> Using a simple example, a forensic examiner is given a digitally signed document and a suspect's public key. The forensic examiner is asked to examine the document and determine if the document was signed using the suspect's private key. The examiner simply must show whether the document has really been signed with the suspect's private key. The examiner's finding would be a simple "Yes" or "No", a decision problem.
>
> In a slightly more elaborate example, a forensic examiner may be given two emails $M_1$ and $M_2$ which are purported to be sent by a suspect S using the S's system to a receiver R. The suspect S admits sending the first email $M_1$ to R but denies sending the second email $M_2$. The forensic examiner's task is to determine if the

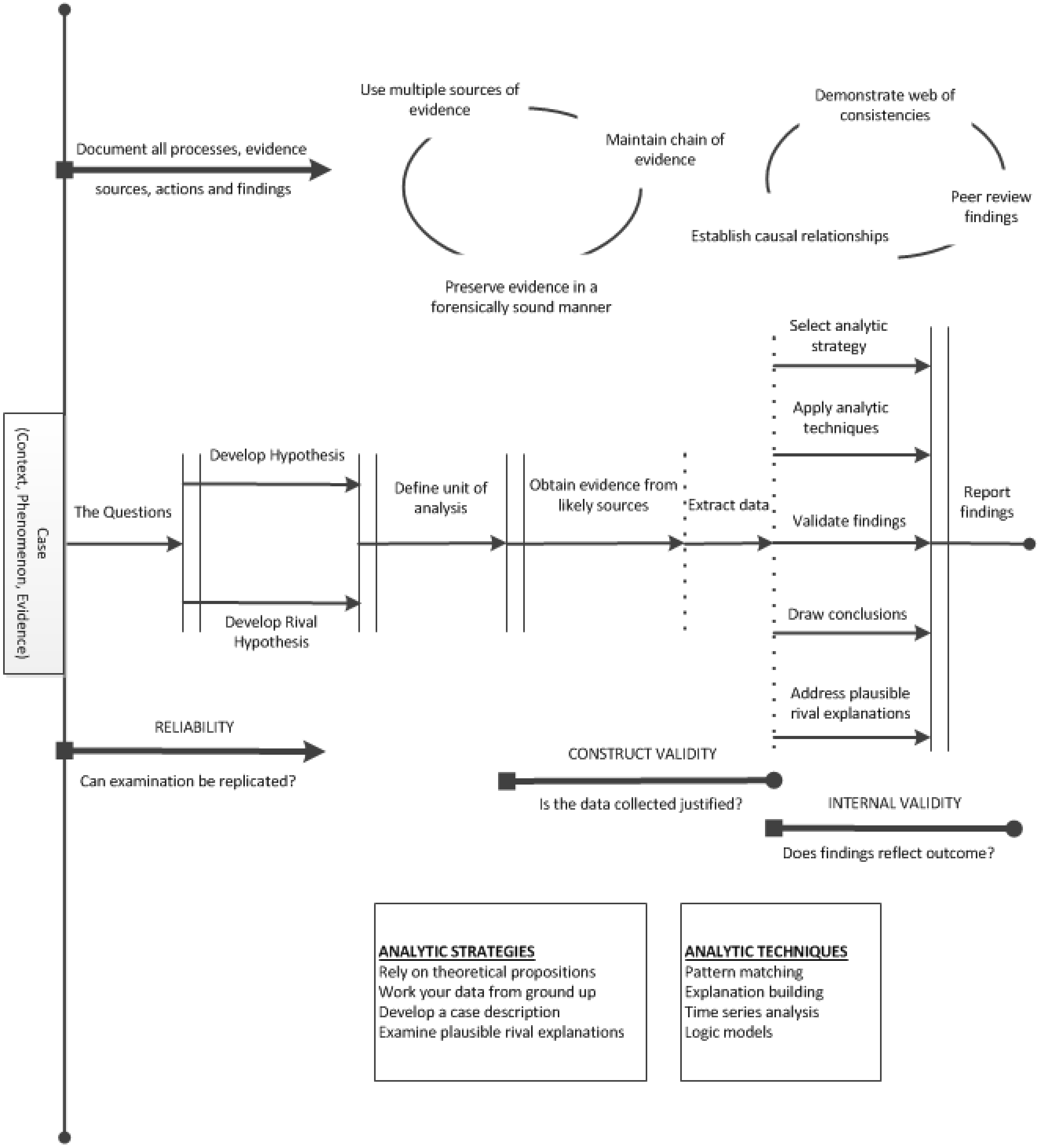

Document all processes, evidence
sources, actions and findings
Use multiple sources of evidence
Maintain chain of evidence
Preserve evidence in a forensically sound manner
Demonstrate web of consistencies
Peer review findings
Establish causal relationships
Case
(Context, Phenomenon, Evidence)
The Questions
Develop Hypothesis
Develop Rival Hypothesis
Define unit of analysis
Obtain evidence from likely sources
Extract data
Select analytic strategy
Apply analytic techniques
Validate findings
Draw conclusions
Address plausible rival explanations
Report findings
RELIABILITY
Can examination be replicated?
CONSTRUCT VALIDITY
Is the data collected justified?
INTERNAL VALIDITY
Does findings reflect outcome?
ANALYTIC STRATEGIES
Rely on theoretical propositions
Work your data from ground up
Develop a case description
Examine plausible rival explanations
ANALYTIC TECHNIQUES
Pattern matching
Explanation building
Time series analysis
Logic models

**Figure 4.2:** Detailed Case Study Design Model.

suspect S sent the second email $M_2$ to R.

The forensic examiner's objective here will be to analyse the email messages and find similarities between the first email $M_1$ and the second email $M_2$. The examiner may request further data such as an image of the suspect's system, mail server logs and ISP logs to make definite findings pertaining to the case. The examiner's findings in this case will not be definite. It will be to the level of certainty by the examiner of the inferences made and the consistency of data examined. The examiner's finding may also be inconclusive which would mean the examiner does not have sufficient evidence to examine the case (mail server and ISP logs deleted, suspect's system not available).

The email example above can be suitably analysed using Yin's approach to case studies. It is a multiple case-study design which is aimed at literal replication. Using the case study approach, our first step will be to define the case study question: How possible is it that these two emails $M_1$ and $M_2$ sent to R did not originate from the suspect S? From this question, we derive our hypothesis that the email messages $M_1$ and $M_2$ were received at R, and allegedly originated from the suspect S. The unit of analysis defines the interest of our research, which is an in-depth study of the two email messages (specifically the email headers) to establish if there are consistencies between them. At this point, the examiner can identify what other sources of evidence are relevant to the case e.g. the suspect's system, the mail server logs and ISP logs of the suspect system. The next step would be to link the study findings or data to the propositions. This is where the analysis of the emails are done and the examiner studies in-depth the email headers of both emails in order to find and establish a web of consistency, the suspect's system to establish if both emails can be found in the mail client specified on the mail header, the server logs and ISP logs to establish if the path the emails followed is consistent with the assertion that the emails originated from the same source computer.

The examiner then considers how he would interpret his results or findings by establishing criteria for interpretation of the case study's findings. Consistencies found in the server logs, ISP logs and the suspect's computer strengthen the findings that the email $M_2$ originated from the same source as $M_1$. While of course, a rival explanation may exist, the task for the examiner is to show that these rival explanations are unlikely or practically infeasible given the strength of the findings. Identifying and addressing rival explanations strengthens the study findings and the more rival explanations are addressed, the stronger the examiner's findings become.

A final example is detailed as follows: In the investigation of a murder case, an examiner is tasked to show the sequence of events that occurred using several witnesses' phone records to demonstrate the reliability of the defendant's version of events. The examiner is presented with a case file containing the facts of the case. The study question can be stated as "How can we show that the phone records of several witnesses provide a sequence of events that is consistent with the version of events as described by the defendant?" Here, we see that the examiner's goal is to determine if in this case, the sequence of events is consistent with the defendant's version. This requires a single case study design approach. The single case design approach requires an in-depth study of the witnesses' phone data to reconstruct the sequence of events.

Next, the examiner defines the study propositions. Based on the study question, the hypothesis may be that the witness's phone records agree with the defendant's version of events. The unit of analysis is to study the phone records of the various witnesses concerned and construct a sequence of events to establish the study propositions. Another relevant source of evidence would be the service providers' call logs, which can be used to confirm the witnesses' call and timestamps. During analysis, the examiner analyses the timestamps on the witnesses' phones, creates a reconstruction of the time lines and establishes its consistency with the defendant's version of events.

Identifying the criteria for interpreting the results is crucial. As discussed earlier in the email case study, explaining inconsistencies found during the analysis stage serves to strengthen the study findings. The witnesses phone clocks may not be synchronised with the mobile service provider's clock and when different mobile providers are involved, the inconsistencies are bound to increase.

### 4.2.5 Documentation on Yin's work on Case Studies

Yin's work on case study research is not an isolated idea. It is widely accepted and has undergone five editions of publication [65] and over a hundred and sixty thousand citations on google scholar. It is important to note that much of what happens in a forensic laboratory already reflects what we understand in the work of Yin. Yin's approach to case studies therefore validates what we as digital forensic professionals do and provides the field with a formal scientific backing. The approach further extends the forensic processes by providing quality indicators for assessing the findings of a digital investigation.

## 4.3 The Virchow Method for Autopsy Examination as a Paradigm

Virchow's method [57] of carrying out autopsies provides a systematic and scientific approach to performing post-mortem examinations. As noted in the introduction to this chapter, the method is the first systematic method developed and is the standard method for performing autopsies from which newer methods have evolved. As in the first section on case studies, a definition of terms is required. The similarity of the terms is also highlighted so the reader may gain insight into the distinct use of terms in the methods.

In an autopsy, the examination's core focus is on the object of investigation. The object of investigation is the corpse to be examined. In normal autopsies, should a patient die while under treatment of some ailment involving a specific organ, the object of investigation may be confined to that organ and other organs may be secondarily observed. An autopsy, also known as a post-mortem examination, is a specialised examination of a corpse that aims to determine the cause and manner of death and the way the death occurred. This is similar to a case study. A prognosis is a statement that speculates the likely cause of death. This is the similar to *a priori* in a case study.

The clinical anamnesis is also called the medical history. It contains information gained by a physician from past interaction with a patient when alive. This information is gained typically by asking specific questions, either of the patient or of people who know the patient and can provide the required information. However, as the focus is on autopsies, this indicates that the object of investigation i.e. the corpse is in no capacity to provide a medical history. For an identified corpse, an history of prior treatment may be obtained. In some cases, such as if the corpse is unidentified, a clinical anamnesis cannot be obtained.

It is important to note that an autopsy is a specialisation of a case study. A case study provides a generalised approach to understanding any occurrence or event while an autopsy is a more specialised approach used to gain insight into the cause of death.

The rest of this section examines the Virchow autopsy method and its application as a specialised forensic science method for determining the cause of death. In discussing this method, the emphasis is on the underlying principles that inform the application of the method in post-mortem examinations.

### 4.3.1 Requirements for Autopsy Examination

An autopsy commences after the death of a patient or an individual. The cause of death may be because of natural or unnatural causes. The aim of an autopsy is to ascertain the cause of death. The first step in this process is to obtain a medical history.

In the determination of the cause of death, there are several considerations and it therefore becomes imperative to provide some context to the process from which a medical history is obtained. While the patient was alive under medical care, the practitioner would determine what organ would be investigated and should the health of the patient deteriorate, and death occurs, an autopsy may be required. In situations where the cause of death was normal or by natural causes, the autopsy would usually be confined to the same organ with a brief examination of other organs. However, should there be evidence that shows that the cause of death may be unnatural, it becomes necessary to examine the corpse in detail as the object of investigation.

The medical history determines the course of the autopsy examination, the questions that need to be answered regarding the object of the investigation. It is important to note that the medical history can only be obtained while the patient is alive. An unidentified corpse will not have a medical history. However, a proper autopsy with or without a medical history, if the corpse is unidentified, would have a prognosis.

The medical history implies the existence of a posteriori (knowledge from previous experience) from which the *a priori* can be developed about the object of investigation - the case - before examination (empirical observation) is conducted. It is therefore important to note that without a correct knowledge of the underlying principles and the body of knowledge of the field, the application of the method would likely yield false results from which incorrect inferences would have been made.

Virchow's method of autopsy examination was designed for medico-legal purposes i.e. examining unnatural death for obtaining evidence and making inferences that can be admissible in the court of law.

Virchow's method relies on two main requirements to ensure and demonstrate the reliability of the findings of the examination. The first requirement is for a complete examination covering the degree of changes in every organ. The second requirement necessitates the examination should be carried out with the utmost care to ensure the least possible disruption to the connection of the parts or organs. This is to ensure consistency in examination and provide certainty that the findings are consistent with the observations as well as the admissibility of evidence for legal purposes. A discussion of these requirements is covered in the rest of this section

The first requirement is for a complete examination covering the degree of changes in every organ. Unlike autopsies for natural death situations where an organ may be the object of the investigation and other organs are subjected to a brief examination, Virchow's method emphasises the completeness of the examination requiring an in-depth examination of the corpse in a methodical manner. This requirement becomes even more relevant should the findings of the autopsy be questioned in aspects relating to other organs. The emphasis on the completeness of the examination ensures important observations are not omitted during the examination.

The second requirement is to carry out this examination with the utmost care that ensures the least possible disruption to the connection of the parts. This requirement places emphasis on the exactness of the method. While examining the organs, the practitioner must ensure utmost care is taken to limit changes to the state or linking of the organs. This is equally important for forensic purposes as there is the need to exercise every precaution in ensuring that the evidence is presented without loss or change at the disposal of the law.

The two requirements discussed above ensure that the method applied is complete and exact. Since a methodical approach presupposes the existence of a definite plan, the insistence of the completeness and exactness of the implementation of the plan guarantees the integrity and consistency of results. However, there will be situations where a deviation from the method is not only required but necessary. In such a situation, the practitioner can alter the course of the examination on well-established grounds while ensuring that the motivation for which such alterations are necessary is well documented.

### 4.3.2 Virchow's Examination

Virchow's Autopsy method can be broadly classified into two parts: external examination and internal examination.

The first part, external examination involves the identification and description of the external state of the object under investigation, that is, the case. The purpose is to reflect the external attributes of the elements of the case. To illustrate this concept, in an autopsy, the external examination would observe the body specifying attributes such as the sex, age, height and structure of the body as well as observations that can be noted on all parts of the body such as the head, hands, face, hair and nails for marks of external injuries specifying attributes such as colour, foreign bodies, condition.

The second part, internal examination involves the dissection of the body in a methodical manner in order significantly examine every organ in detail while ensuring the least disruption in the connection of the organs examined. In situations where the practitioner may deviate from the methodical approach required by Virchow's method, this deviation is allowed and may be necessary based on the uniqueness of the case under examination. The practitioner should, however, be able to support logically with well-grounded motivation the rationale for deviating from the method. The most important and most difficult step in the scientific performance of an autopsy is the reasoning and motivation behind the decision to follow a set of processes in every aspect of the examination.

An equally important step in Virchow's method is the need to document the examination process as well as the reasoning process that motivated the selection of the procedures used in the examination. Following a prescribed approach not only guarantees completeness and prevents the omission of important aspects of the examination, it also ensures that a repeatable, reliable documentation of the examination can be collated in a manner that reflects a methodical approach.

## 4.4 Exploring the Methods

The case study method is a scientific method, an approach that is generalised for examining an occurrence or phenomenon. Virchow's method on the other hand is a specialised forensic science method specifically designed for examination during autopsies. Both methods, however, focus on achieving the aim of establishing reliable findings about the cause of a specific occurrence using approaches that are methodical and grounded on a scientific body of knowledge.

This section provides a preliminary exploration of the two methods in tandem with a view to derive a methodical approach that further contributes to the examination of occurrences in such a way that advances the certainty of findings for forensic examinations

As the reader may have now realised, an autopsy is really a case study. The logic that the autopsy method implements is very similar to that of the case study method. The issues that underlie a case study also underlie the autopsy method and it is important to note that the goal of the autopsy method maps to the goal of the case study method. An important goal is to ensure completeness and exactness of the method as well as to eliminate bias and errors in the examination. Each of these aspects are explored in this section.

Logic implies a structure, a course of action or a definite plan that guides the implementation of a system or method. Logic enables valid reasoning and deductions to be made when examining an occurrence. Methods, i.e. Virchow's Autopsy and Yin's Case study method, implement very similar logic in the examination of an occurrence.

In a case study, questions are asked of the occurrence from which hypotheses are made that need to be tested. The questions in a case study maps to what is obtained from a clinical anamnesis. As indicated earlier, an unidentified corpse would not have a clinical anamnesis. Whether or not a clinical anamnesis is made, the main question of the autopsy is to determine the cause of death. Therefore, a prognosis can still be made about the object under investigation.

The case study method introduces the logic of replication using several techniques and strategies. The idea of replication logic provides the examiner with the ability to test the study hypothesis using literal replication and disprove rival hypotheses using theoretical replication. The whole idea is based on establishing causal relationships using multiple sources of evidence and ultimately showing consistency, or a web of consistency that supports the hypothesis in the case.

The case study method employs several analytical strategies and techniques. An obvious analytical strategy employed in the case study method is to focus on proving the hypothesis. A second analytical strategy is to work the data from the ground up. Using this strategy, the examiner analyses data to find interesting patterns and traces within the evidence. This strategy is interesting as it maps to the logic employed by Virchow's method. Virchow's method studies the object of investigation on an organ by organ basis in a systematic order. Each organ is observed covering the degree of changes while it is necessary to ensure the least disruption to the connection of the parts or organs.

Virchow's method further provides unique insight into an aspect of the logic used in the method which illustrates the issue of completeness and exactness of the method. In the examination of an autopsy, it may be necessary to deviate from a predetermined course of action. Such a deviation is allowed. Furthermore, he states that "In a systematic and scientific performance of an autopsy, nothing is more difficult, and at the same time more important than the insight into the reasons for pursuing a definite order of sequence in every detail of the examination" [57]. This implies that the reason for a practitioner's decision for taking a course of action must be supported by valid reasoning and documented.

To ensure completeness and exactness of the method, the case study method employs the use of validity tests: Construct validity, Internal validity, External validity and Reliability. The use of criteria for interpreting the findings of the analysis also supports the completeness of the method. One of these important interpretation criteria is the addressing of rival explanations that do not support the hypothesis of the study. The more rival explanations are addressed and excluded, the stronger the findings and inferences made from the examination.

The goal of the methods is implicit: To present a consistent complete examination of the case or object of investigation. To determine the cause and possible attribution of causes in relation to the effect observed. To ensure consistency of results and the reliability of findings made from the examination.

The case study method and Virchow's autopsy method have similar logic but also together can provide more consistent results when employed in the examination of occurrences.

## 4.5 Summary

This chapter provided a description of two methods, a scientific method and a forensic science method that can be applied as paradigms to incorporate scientific principles and actions in a forensic process. Of utmost importance in both methods is the need to follow a methodical approach, the specifying of *a priori* that provides a focus for the examination and the documentation of the processes carried out within the examination process. The need for a methodical examination cannot be over emphasised. An unmethodical approach greatly limits the subsequent documentation of the examination. An unmethodical approach obliterates the existent condition of the parts of the object under investigation. An unmethodical approach to an examination will undoubtedly yield errors and ultimately, the opinions based on these results will be false.

In the next chapter, the focus will be on developing and applying a conceptual framework based the principles presented in this chapter to examining digital evidence. The next chapter applies the principles and techniques derived from the case study research method to digital evidence examination and demonstrates the suitability of case study research as a scientific basis for digital forensics.

# Chapter 5

# A Framework for Digital Evidence Examination

Chapter 4 provided an introduction to Yin's approach to the case study method and Virchow's method of autopsy examination. Yin's case study method was explored as a general method of scientific inquiry and Virchow's autopsy method, as a specialised forensic science method. The intricacies of applying the methods and their use as paradigms for digital forensics were also examined. Virchow's method of autopsy examination was observed to essentially illustrate a specialised method of case study examination.

This chapter examines the application of the case study method as it relates to digital evidence examinations. The approach is to apply the principles and techniques derived from the case study method in the examination of digital evidence. Several concepts are defined in this chapter to provide context for digital examinations. This chapter aims to adapt the principles and techniques derived from the case study method to digital forensic science and demonstrate the viability of the case study method to digital forensic examinations. As noted earlier, the highest state of inference in a digital examination is determining causality as it relates to observed phenomenon. As such, this chapter commences by examining causality and its intricacies and goes on to apply the concepts adapted from the case study method for conceptualizing digital evidence examination using case studies.

Causality is about drawing relationships between an observed phenomenon - effect -

and its cause(s). The effect is the evidence under observation. In forensic examinations, establishing these relationships implies proof and validity of the findings of a forensic examination. In establishing cause and effect relationships, a forensic examiner analyses evidential data obtained from the evidence and identifies patterns within the data that may be used in establishing different paths or relationships for evidence attribution. An understanding of the patterns within data and their application in establishing or refuting hypotheses made by a forensic examiner is central to establishing the findings of the forensic examination.

To demonstrate causality, a forensic examiner will look for consistencies within the evidence. Consistencies found provide validity of causal findings made during examination. These consistencies ultimately form a web of consistency which provides proof for the findings of an examination. A web of consistency provides proof that supports the facts of the findings and validates supporting information that validates or invalidates the hypothesis made by a forensic examiner. The concept of establishing a web of consistency is further supported by Casey's certainty scale [8] which notes that evidence supported by multiple independent "and verifiable" sites have a higher certainty value than information obtained from a single source that may have been tampered with.

This chapter presents a framework for examining forensic evidence by applying the case study method in establishing a web of consistency within forensic evidence and ultimately demonstrating causality. Section 5.1 provides a brief introduction to cause and effect as it relates to digital forensic examinations. Section 5.2 derives concepts and ideas from Yin's case study method and Virchow's method of autopsy examination and applies these concepts to develop a framework for examining digital forensic evidence using the case study method. Section 5.3 further reinforces the concepts of causality in digital systems and applies the framework in example digital occurrences. Section 5.4 concludes the chapter.

## 5.1 Nature of Cause and Effect

Evidence exists in different forms. Locard's principle on the transfer of evidence stipulates that the act of committing a crime leaves traces or artefacts at the scene of the crime [24]. It is also possible that artefacts are also taken from the scene of the crime. In digital systems, Locard's exchange principle also holds. A digital crime leaves traces on several systems and on the systems from which the crime was committed. This section explores the nature of cause and effect in relation to digital evidence.

#### Cause - The Source of Evidence

A cause triggers an effect. An effect may have several plausible causes. These plausible causes provide rival explanations that explain an observed effect. Establishing the real cause from several plausible causes is essential to establishing the findings of the examination.

#### Effect - The Evidence

An effect is an observed phenomenon, the evidence that reveals an occurrence or a crime. An effect can be observed in two forms namely actively or passively. An active effect reflects the main occurrence, which can usually only be observed while it is happening. In most cases, active effects are transient. A passive effect reflects the trace or side effects that are due to the occurrence of the active effect.

## 5.2 Forensic Evidence Examination

Chapter 4 provided an approach for examining phenomena using the Case Study method and Virchow's method of autopsy examination. This section brings together concepts and ideas from the application of these methods for conceptualising digital evidence examination.

### 5.2.1 The Examination Process

The process of carrying out a proper forensic examination involves several aspects to ensure the reliability of the findings of the investigation. Three aspects that may determine the outcome of a forensic examination process are the forensic examiner's experience and knowledge of the field of expertise in which the evidence is being examined; the formulation of the hypotheses of the forensic examination and the testing of hypothesis of the examination. These three aspects impact on the reliability of the findings of a forensic examination and are explored in this section.

### The Body of Knowledge

The first aspect requires a forensic examiner to have the experience and scientific knowledge of the forensic field to practice within that field. The understanding of the body of knowledge of the field is a necessary requirement for all forensic science disciplines [24][36]. An examiner must have expert knowledge of the field in which the examination is intended to be carried out. Without expert knowledge of the field, an examiner cannot consistently make valid claims, nor will the hypothesis be based on the body of knowledge and experience gained from the scientific practice within the profession.

### Hypotheses Formulation

The second aspect is the development of hypotheses. The formulation of a hypothesis is based on the questions that are asked about the evidence. Hypothesis formulation plays an important role in the examination of evidence. The process of formulating the hypotheses also guides the examination phase. As earlier noted in 4.2.1, hypotheses are typically developed in sets with one of them being the main hypothesis and the other, the rival hypothesis. The main hypothesis reflects what the examiner expects to observe and demonstrate within the context of the examination. Rival hypotheses are plausible explanations that oppose the main hypothesis and are required to be disproved.

In forming a hypothesis, an examiner typically would seek to explore one or two main forms of questions during the examination of evidence. In its first form, the examiner may be required to address a decision problem [39]. In its second form, the requirement is to address a narrative problem [46] [47]. The decision problem addresses the examination of evidence in terms of the main hypothesis.

For example, “Do these fingerprints match?” A generic decision problem in digital forensics may be stated as “Does this pattern occur on the disk?” where the pattern may refer to a software signature, execution of a malicious software, a downloaded software or evidence of an intrusion or compromise on a network. A decision problem usually produces a definite result, that is, a "yes" or a "no". The narrative problem on the other hand addresses the examination in terms of causality. For example, "what is the cause of death?" A generic formulation of a narrative problem in digital forensics is "what caused this pattern to occur on the disk?" where the pattern is as illustrated above. To further explore the use of decision problems and the narrative in digital forensics, these cited publications [39] [46] [47] may be of interest to the reader.

The formulation of hypotheses may take any of the two forms discussed above. While a narrative problem may also be interpreted in the form of a decision problem, both forms serve different purposes but also achieve the same goal of explaining the findings made from the evidence examination. The formulation of hypothesis should be done before examining the evidence to ensure that the examination is free of bias and errors [36] [40] and provides a focus for the examination of the evidence.

### Hypothesis Testing

This leads the forensic examiner to the third aspect which is the evidence analysis phase. The main purpose of this phase is testing the hypothesis made by the forensic examiner.

In testing a hypothesis, an examiner examines the likelihood of an occurrence reaching a definite conclusion. In the example where the question "Does this pattern occur on the disk?", the examiner may seek to demonstrate the occurrence of the pattern on the disk. The result may be a "yes" or a "no" which is a definite result. However, the result may also be a "maybe" indicating that what is observed does not provide sufficient proof to confirm or deny the plausibility of the pattern occurrence. This may occur in cases of file deletion, evidence tampering and so on.

The question "what caused this pattern to occur on the disk?" examines the occurrence in terms of causality. The examiner may seek to demonstrate that the pattern is attributable to a certain cause - confirming the hypothesis. However, in doing this, the examiner must also actively identify evidence that refutes this hypothesis. An examiner may successfully be able to show that a certain effect is attributable to a cause. However, to reinforce the finding, an examiner is required to refute other plausible rival explanations.

To ensure the reliability of the findings, a methodical approach must be applied analysing the evidence, establishing causal relationships and demonstrating a web of consistency between the evidence and its plausible causes. There are several strategies and techniques that can be applied. These techniques are pattern matching, explanation building, time-series analysis and logic models briefly discussed below. Also, for multiple case studies, an examiner may use the cross-case synthesis technique which applies the logic of replication namely literal replication and theoretical replication.

The pattern matching technique enables an examiner to compare predicted patterns or hypotheses made before examination against observed patterns. Predicted patterns are hypotheses specifying expected findings made based on the body of knowledge about the occurrence.

The explanation building technique enables an examiner to develop a narrative of the case by specifying a set of causal relationships about the occurrence or explaining "how" and "why" the occurrence happened. This involves making an initial hypothesis or explanatory statement about the case, then testing the explanatory statement and revising it to reflect the new findings within the case. The revised explanatory statement is then tested again as new findings are made in an iterative manner until an explanatory statement is made that fully reflects the final findings of the case.

The time-series analysis technique enables an examiner to observe an occurrence bringing together key aspects of the occurrence in a chronological order as it happened over time. The chronology also reflects the case as a set of causal relationships showing which aspect caused or contributed to the existence of the other aspect of the case.

The logic model technique enables an examiner to break down complex occurrences into repeated cause and effect patterns which demonstrate how the final findings were made from intermediate findings within the case.

Another technique which is equally important is the cross-case synthesis technique, mainly used in multiple case examinations. This technique applies the logic of replication which has two sides: literal replication and theoretical replication. By using literal replication, an examiner can select several cases to demonstrate similar findings. This also provides a web of consistency. Theoretical replication enables an examiner to select and examine another set of cases while predicting opposing results and invalidate them.

Whatever strategy or combination of strategies are employed in examining a case, an examiner must take note of and address plausible rival explanations found within the case. To achieve this, an examiner must also collect data on possible rival explanations and examine them to demonstrate their unsuitability. Using the explanation building technique, an examiner must build in an explanation to rival explanations as the case is explored. Using the time-series analysis technique, an examiner can show that the rival explanation does not fit the chronological pattern and therefore is unsuitable to explain the case. Also using the logic model technique, an examiner can demonstrate that rival explanations cannot be reached from intermediate findings.

The goal of addressing rival explanations is to demonstrate the unsuitability of the rival explanation in sufficiently explaining the case. The refutation of rival explanations reinforces the findings of a case. It also validates the examination by demonstrating the design of the examination followed a methodical approach that is based on science.

The next section focuses on establishing causal relationships. The process of establishing causal relationships conceptualises this analysis phase of evidence examination.

### 5.2.2 Understanding Causal Relationships

Drawing relationships between a cause and its effect requires identifying patterns during the analysis of evidential data. Patterns that are found can be applied in establishing and demonstrating different relationships. These relationships may take several forms such as correlations, consistency in data and plausible causes. Relationships that form correlations are patterns that reflect matching data within the evidence. Consistency relationships are patterns that posit a cause or plausible causes on an effect. Plausible causes are several likely mechanisms or actions that can initiate the effect and as such may have initiated the effect.

For example, a valid user name and its corresponding password have a correlation as a login credential. A relationship that demonstrates consistency may be, for example, a successful login attempts to a website which reflects a valid user name and a corresponding password entry within the database was applied. However, a successful login attempt to a website may also be executed by a SQL injection mechanism captured in the database log which enabled access to login information. The plausible causes of the successful login to the site are as such the use of an SQL injection mechanism and the use of valid login credentials. Though the SQL injection mechanism initiated a successful login via the use of valid login credentials, both actions produced effects on the system.

Using matching data, an examiner can posit that an action was taken causing an effect to occur. This indicates that correlations support the claim for consistency and this implies that consistency claims have a higher order in establishing causes. From correlations, consistency claims can be established, and these claims can be applied in demonstrating causal relationships or causality. The next section explores concepts that support the establishment of causal relationships.

### 5.2.3 Establishing Causal Relationships

The process of establishing causal relationships supports the proving of the hypothesis. It also strengthens the claims of causal inferences that are made by the examiner. In a forensic examination, there may be several causes that can trigger an effect. An examiner may be required to show that a certain cause is the main cause by demonstrating its plausibility and the strength of the correlation and consistency patterns that support the claim of causality. The following discusses three main concepts that support the establishment of causal relationships. These concepts are the specification of the necessary and sufficient conditions for causality, establishing a web of consistency within the evidence and refutation of rival hypotheses or explanations.

#### Specification of the Necessary and Sufficient Conditions for Causality

An effect may occur under certain conditions, and several conditions may be necessary for the effect to occur. The existence of causes may not be indicative that all the plausible causes contributed to the effect. A certain cause may be considered sufficient to initiate an effect without the participation of other conditions or causes. Thus, an examiner may be required to determine which cause(s) contributed to the effect being observed from two or more plausible causes. The examination may further determine under what conditions the effect would be rendered implausible. A condition X is said to be necessary for an effect B to occur if and only if the falsification of the condition X guarantees the falsification of B. A condition X is said to be sufficient if its occurrence guarantees the effect B will occur. Therefore, necessary conditions are the conditions without which an event cannot happen, and sufficient conditions are the conditions that guarantee an expected outcome.

To illustrate this concept using a simple example, to delete a file, a system may support a DEL command, an rm command or any other command that enables the file to be deleted. The execution of any of these actions can cause a file to be deleted on the system. However, a user attempting to delete a file while having a read-only permissions on the file would be unable to do so as the necessary conditions or pre-conditions required for a deletion to occur have not been met. This implies that an appropriate user access right and an appropriate command to delete are necessary conditions for deleting a file. An administrator or super user on the other hand has full control of a system and in this case, a DEL command would be sufficient to delete the file.

In establishing causal relationships, an examiner may be required to show proof that a certain effect can be attributed to a cause. By demonstrating that all the conditions existing are sufficient for the effect to occur, an examiner can corroborate the claim that the effect was as a result of the cause. A plausible rival explanation may be eliminated or at least considered doubtful by showing that one or more conditions that are considered necessary for the effect to be considered attributable to the rival cause are not found.

Using another example, suppose X implies visiting a web page, the side effects of X may be the HTML file displayed on the screen, followed by subsequent connections to retrieve images for the page and then followed by requests for linked web pages. In addition, the action of X may also cause a log of the source IP address to be written on the web server, and a log of the web page in the browser web history and the file may be cached at the source system and so on. Suppose then that X and Y are two events where a web page was visited, and a defendant confirms X and denies Y. It is sufficient to show that Y occurred if the examiner can show that the conditions necessary for Y to have occurred are observed and the effects that can be attributed to the occurrence of Y are also observed. The demonstration of these conditions establishes a web of consistency within the evidence that show that what is claimed is backed by multiple sources of evidence which corroborate and reflect the findings of the examination. A finding made in an examination without the necessary condition of the hypothesis being met refutes the validity of the hypothesis.

### Establishing a Web of Consistency

A web of consistency is established when the evidence from various sources are found to corroborate and therefore form a convincing argument for the claim for which the findings are made. The specification of the necessary and sufficient conditions of a case supports the establishment of a web of consistency. The more tightly coupled the evidence found within a case are, the less likely that there will be several plausible causes. This reinforces the certainty of the findings based on the attribution of events.

Using the example above of the defendant denying a webpage Y was visited, establishing a web of consistency requires that network devices such as firewall, proxy and intrusion systems within the network have activity logs that validate the web page visited. Examining the user device may also provide evidence of the browser web history, web cache, search history, cookies and web beacons which store information about the user's online activities. However, if evidence is not found, it may be likely that the user may have cleared the browser cache and deleted the web history. The examiner may then be able to show that that data deletion occurred. The examiner expects to see traces or signs of deletion to make justified inferences about the case. In the case that there are limited or no traces, justified inferences cannot be made about the case.

### Refutation of Rival Hypothesis or Explanations

In examining a case, plausible rival explanations may be found that usually also explain an occurrence contrary to the main hypothesis. These explanations may be eliminated or at least considered doubtful by demonstrating that one or more conditions that are considered necessary for the effect to be considered attributable to the rival cause are not found. A statement by Campbell [65][64] demonstrates the significance of rival explanations in the examination of occurrences. Campbell [65][64] noted that *"More and more I have come to the conclusion that the core of the scientific method is not experimentation per se, but rather the strategy connoted by the phrase, 'plausible rival hypothesis' "*.

Addressing rival explanations can be used as a criterion for interpreting the findings of an examination. Rival hypothesis must be addressed to strengthen the findings of an examination. The examiner must be able to demonstrate that a certain rival cause does not fully address the conditions that are present within a case and therefore cannot be an attributable cause. This provides a more convincing argument for the findings of the case. The more rival explanations are addressed and excluded, the stronger the findings of the examination.

In establishing causal relationships, the specification of the necessary and sufficient conditions for an effect to occur, the requirement to establish a web of consistency and the examination of rival explanations enables an examiner to test the hypothesis and validate the findings of an examination. The next section examines how case study method can be applied to the examination of digital systems.

## 5.3 Applying the Framework to Digital Systems

A digital system is made up of a complex set of programs that are executed within a system. These software programs are executed and controlled by the programs' control logic. The control logic is an important part of a program that executes and controls the operations of the program. The control logic processes commands passed by a user and executes the commands on the system. It also controls and executes automated operations that have been structured into the software program.

The execution of input commands and/or automated operations by the control logic causes its effect in the system. This implies that the control logic is the cause in the system. The control logic triggers its effect. The effect triggered by the control logic may be an active effect or a passive effect. A passive effect occurs when the execution of the control logic causes traces or side effects in the system. In other words, passive effects are known as traces or side effects in the system. On the other hand, an active effect occurs when the execution of control logic triggers further control logic executions in the system. The further executions of control logic are active effects within the system but may also leave traces or side effects which are passive within the system. An illustration is shown in Figure 5.1

In Figure 5.1, a cause C leaves a passive effect or trace $T_1$ and its execution triggers an

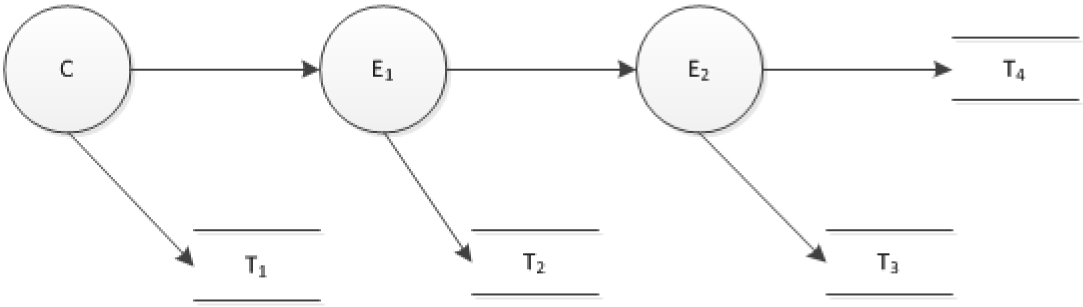


**Figure 5.1:** An illustration of Cause and Effect in a Digital System.

active effect $E_1$. The initiation of the active effect $E_1$ leaves a trace $T_2$ and its execution triggers another active effect $E_2$. The initiation of the active effect $E_2$ leaves a trace $T_3$ and the execution of the active effect $E_2$ also leaves a trace $T_4$. As illustrated in Figure 5.1, an effect can be an active effect, or it may be a passive effect which is a trace in the system. The active effects - the execution of the program control logic is transient within the system. This indicates that active effects are not observable because the execution of a command is invisible in the system. What can be observed in the system are the traces or effects of commands executed on the system.

To further illustrate the concept of cause and effect in a digital system, consider the following examples.

**Example 1: Execution of a Bash Shell Command.** An example of this concept is the execution of a bash shell command initiated when a certain input was passed by a user. The input passed to the bash shell is stored in the bash history and execution is initiated by the control logic. An examiner knows that the control logic initiated the bash shell command because of the traces of the command left in the bash history. The execution of the bash command is however invisible and leave no traces therefore it is not possible to know if the command did execute. It is also possible that environmental variables may have been configured to disable the bash history. However, programs that execute may leave traces and an examiner can conclude that the program caused those traces.

**Example 2: Crontab File Execution.** A second example is the execution of a crontab file. A crontab is a system service that causes commands to be executed at specified times. The execution of the crontab is controlled by the cron daemon, the control logic which executes the commands in the system background. When the specified time for a command execution is met, the cron daemon initiates the command, and passively logs the initiation of the command. The logging of the crontab command is a passive effect while the execution of the command is the active effect in the system. The command may or may not, however, have been executed and may not leave any traces within the system. There may be passive effects to indicate success or failure in execution and there may not be any effects to indicate whether the execution was successful or not.

**Example 3: Execution of a Database Trigger.** A third example is the execution of a database trigger. A database trigger executes a sequence of commands when a logical condition is met. The initiation of the database trigger may create a log entry, a passive effect and its execution may create another log entry and may also initiate another trigger, which is an active effect and may in turn cause a log entry.

**Example 4: Email arrival at a Mail Transfer Agent.** A fourth example is the arrival of an email at a Mail Transfer Agent (MTA). Email is forwarded from one MTA to the next until it is delivered to the recipient's inbox. The arrival of an email at a MTA causes a log of the email communication to be written, a passive effect, and the email is then routed onwards to the next MTA in the delivery path or delivered to the mailbox of the recipient. The routing of the email is an active effect while the delivery to the mail box of the recipient is a passive effect.

Drawing inferences from the above examples, the arrival of the email at the Mail Transfer Agent (MTA) in example four is almost similar to the bash shell interface waiting for a command from the user. This is also similar to the cron daemon waiting till the time arrives to execute a command from the crontab and this is also similar to a database watching the data and waiting for a condition to be met to execute an operation. From these, it is possible to conclude that the command entered in example one, the logical conditions met in examples two and three and the email that arrived at the MTA in example four are all forms of input to the system that cause the control logic to take a specific course of action.

In conclusion, the control logic waits for an input which may be a command that is typed or a logical condition that is met, and the arrival of the input may cause a passive effect and may also cause an active effect within the system. It is important to again note that observing passive effects on a system does not imply that an active effect, a command execution occurred, it only implies that the command was initiated. If, however, the execution of the command leaves traces on the system, then the traces can indicate the command was executed on the system.

### 5.3.1 Notion of Causality in a Digital System

A digital system operates on a pre-set mode of execution, the system configuration. It is also programmed to accept certain inputs into the system and depending on what input is received, the program control logic executes the expected sequence of commands pre-defined by the system. Depending on the configuration of a system, certain traces are typically left in the system. This implies that from the system configuration and known inputs, an examiner may be able to predict what traces may be found on the system. This can be described as the forward motion of causality. On the other hand, an examiner may also be able to predict based on the traces found on the system, the system configuration and the input to the system at the time. This can be described as the backward motion of causality. This concept is illustrated in Figure 5.2.

In applying the notion of causality in a digital system to a forensic examination, the forward and backward motion of causality are applied as illustrated in Figure 5.3. A forward motion allows an examiner to predict what traces are expected based on the system configuration and program input. The backward motion enables an examiner to predict the plausible causes within the system. Again, note that an input may be a command that is typed into an interface or a logical condition met which satisfies the requirement for the execution of a database trigger. Based on the predictions made

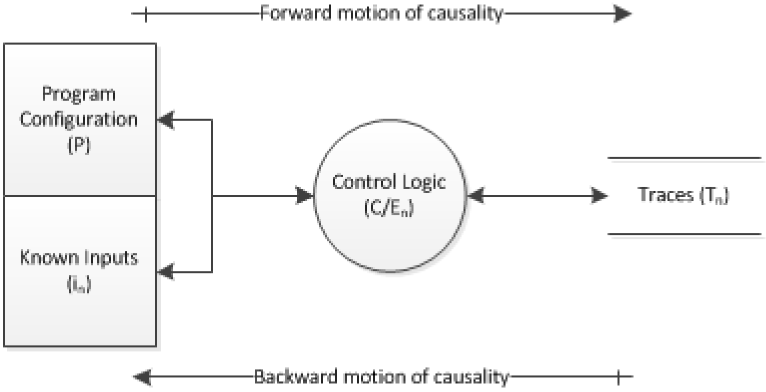

Forward motion of causality
Program Configuration (P)
Known Inputs ($i_n$)
Control Logic (C/$E_n$)
Traces ($T_n$)
Backward motion of causality

**Figure 5.2:** An Illustration of the Forward and Backward motion of Causality in a Digital System.

from the traces using the backward motion, an examiner can test the plausible causes to demonstrate causality. This is again applying a forward motion in hypothesis testing. This process is depicted in Figure 5.3.

In formalising the notion of causality in a digital system, a formal definition of cause and effect is required in the context of a digital system. As earlier noted, the control logic is the cause. The control logic requires an input to initiate an effect in the system. An effect may be passive or active. An active effect occurs when the execution of program control logic initiates further control logic executions within the system. A passive effect is a trace within the system which is as a result of the initiation of control logic within the system.

Based on the above, the notion of causality in a digital system is defined in terms of its forward and backward motion.

**Definition 1: Notion of Causality in a Forward Motion.** *A cause, based on an input, may initiate its passive effects and the initiation of its active effects. The execution of the active effect is a cause which may further initiate passive and/or active effects within the system.*

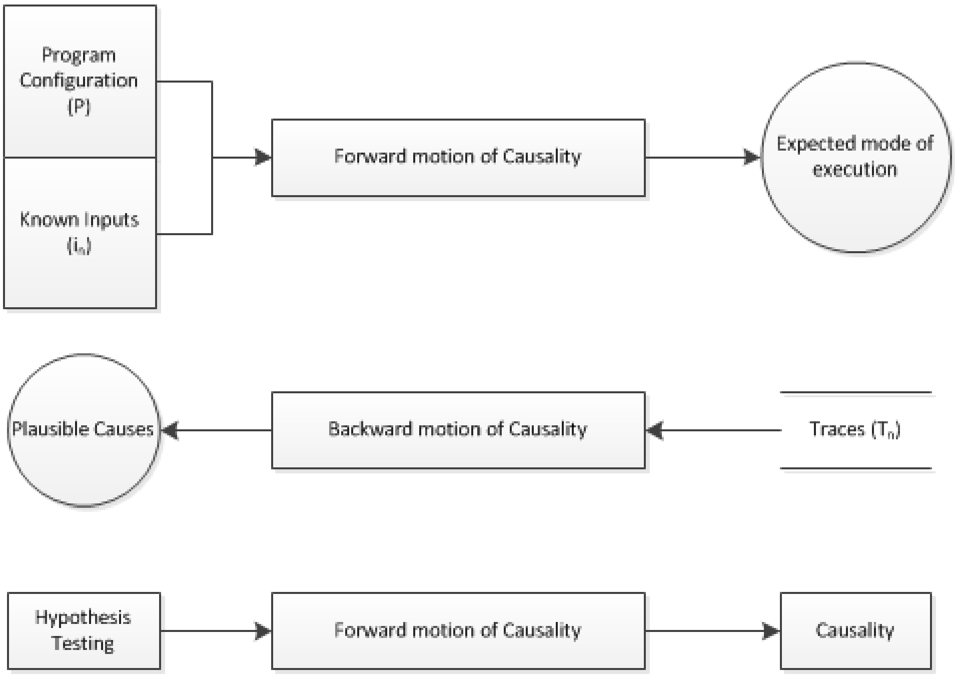

Program Configuration (P)
Known Inputs ($i_n$)
Forward motion of Causality
Expected mode of execution
Plausible Causes
Backward motion of Causality
Traces ($T_n$)
Hypothesis Testing
Forward motion of Causality
Causality

**Figure 5.3:** An Illustration of the Forward and Backward motion of Causality as applied in Forensic Examinations.

**Definition 2: Notion of Causality in a Backward Motion.** *From traces, the execution of a cause, i.e. the control logic, may be predicted. The initiation of this cause may be from one or more inputs or may be an active effect of another cause that has its own traces and/or causes within the system.*

The notion of causality in its forward motion defines a view of a digital system in terms of its expected mode of execution. This enables a forensic examiner to predict what traces are expected when program control logic initiates an execution. The forward motion of causality is also applied in testing the plausible causes that the examiner determined may have occurred based on the traces found in the system. The backward motion defines a view of a digital system that allows an examiner to determine the activities of a system after the fact. This is emphasised by the fact that when a digital system is examined, what are mainly examined are the traces. The notions of causality in its forward and backward motion together formalise causality in a digital system.

### 5.3.2 Forensic Examination of a Digital System

In examining a digital system, a forensic examiner analyses the effects on the system. As noted earlier, active effects cannot generally be observed as a forensic examination usually commences after the fact. Therefore, what are examined are the passive effects which are traces or side effects left in the system. In a live digital forensic examination, it may be possible to observe active effects within the system. In examining traces in a digital system, the forensic examiner can determine, based on the traces found, that certain events may have occurred. From the traces, a forensic examiner may be able to predict what active effects may have been executed on the system. The rest of this chapter examines how a methodical approach can be applied in demonstrating causality when examining digital systems for forensic purposes. The next section illustrates the determination of causes using a real-world scenario of a Lottery Terminal Hack [50].

#### Case Study: The Lottery Terminal Hack

The determination of causes is an important task in digital forensics as demonstrated using the following real-world case of a Lottery Terminal Hack [50]. This incident involves the manipulation of a lottery game system known as 5 Card Cash. The 5 Card Cash game [32] is a digital 52 card playing deck system based on a standard poker game that generates a ticket containing five randomly selected cards. This allows a player to win up to two times. The first win is an instant prize based on the card composition on the ticket. The second win is when the lottery draws five cards from the deck each evening and a player can match the ticket with two or more of the randomly drawn cards. The real-world investigation of this incident is summarised, and the incident is examined as a case study.

***The Case***

The 5 Card Cash game was suspended after it was suspected that the lottery game may have been manipulated. It was observed that the game winnings were excessively higher than the game's parameters should have allowed.

### *The Investigation*

> *"An investigation determined that some lottery retailers were manipulating lottery machines to print more instant winner tickets and fewer losers . . .*
>
> [. . . ]
>
> *An investigator* [. . . ] *determined that terminal operators could slow down their lottery machines by requesting several database reports or by entering several requests for lottery game tickets. While those reports were being processed, the operator could enter sales for 5 Card Cash tickets. Before the tickets would print, however, the operator could see on a screen if the tickets were instant winners. If tickets were not winners, the operator could cancel the sale before the tickets printed."*

### *Examining the Lottery Hack Incident as a Case Study*

The examination in this case will be focused on testing the inferences made by the investigators. This will be done by examining the case and applying the principles and techniques in the case study method. The goal is to demonstrate using this method how the inferences may have been determined and with what certainty the inferences can be considered reliable.

As the case itself does not provide much information about the design of the 5 Card Cash game, a generic design of such a game will be used to illustrate the examination and assumptions will be made about the workings of the 5 Card Cash system. Figure 5.4 provides a topology of the 5 Cash Card game.

To provide the context from which the examination can commence, a generic program configuration is provided in Figure 5.5 displaying the components that make up the system.

The system has six components which perform different functions such as generating lottery tickets, processing payment for tickets, printing tickets as well as generating reports. From the diagram, one can observe that the output of a system component

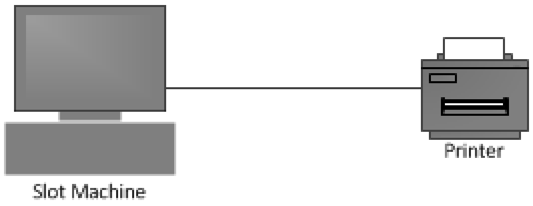


**Figure 5.4:** Topology of a 5 Cash Game System.

may also be the input to another component in the system. This implies that certain components of the system must be executed before another component may be able to start its execution. For instance, a ticket must be generated before it can be displayed or printed. Reports also must be generated before they can be printed.

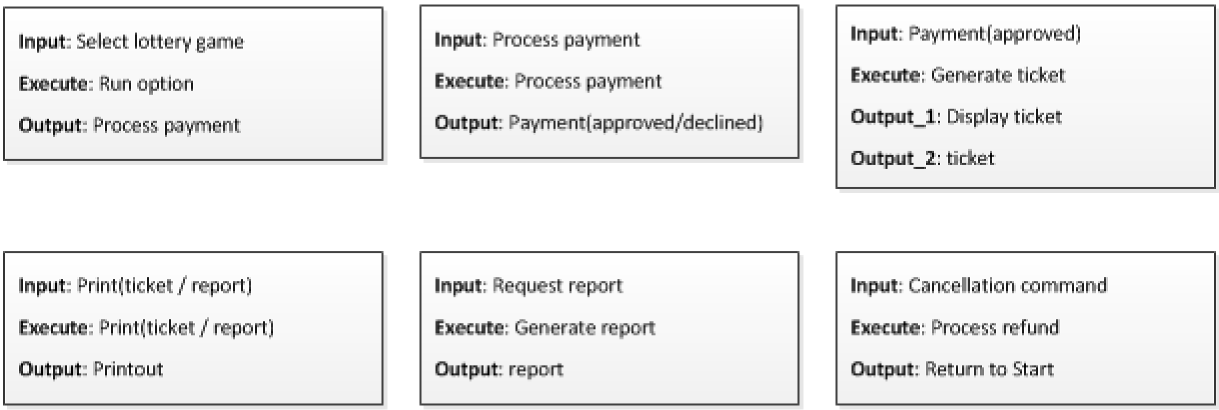
### *Formulating the Study Hypothesis*

From the investigation as explained above, the questions that the examiner may likely be asked can be framed as a decision problem and a narrative problem. As stated earlier, the decision problem addresses the examination in terms of the hypothesis of the study and the narrative problem addresses the examination in terms of causality. The decision problem and the narrative are stated as follows:

> *Decision problem.* Are transactions deliberately cancelled after the results are known?
>
> *Narrative problem.* What enables the cancellation of transactions after the results are known?

The case study based on the above questions tests the following hypothesis.

> . . . the hypothesis that the terminal was manipulated to display the results in a way that would allow the operator an undue advantage in determining favourable results and enable the cancellation of unfavourable transactions.



**Input**: Select lottery game
**Execute**: Run option
**Output**: Process payment

**Input**: Process payment
**Execute**: Process payment
**Output**: Payment(approved/declined)

**Input**: Payment(approved)
**Execute**: Generate ticket
**Output_1**: Display ticket
**Output_2**: ticket

**Input**: Print(ticket / report)
**Execute**: Print(ticket / report)
**Output**: Printout

**Input**: Request report
**Execute**: Generate report
**Output**: report

**Input**: Cancellation command
**Execute**: Process refund
**Output**: Return to Start

**Figure 5.5:** Program Configuration of a 5 Cash Game System.

The expected outcome of testing the hypothesis is to confirm its claim. To do this, the examination must be able to demonstrate that unfavourable transactions were cancelled after the results were known and that transactions which were considered favourable were not cancelled after the results were known.

The rival hypothesis is that the terminal was not manipulated in any way and the game's winning are the result of legitimate transactions obtained within the scope of the game's parameters.

### *Testing the Hypothesis - Case Analysis and Interpretation*

Based on the program configuration in Figure 5.5, an examiner can depict the system as a cause and effect pattern or logic model as shown in Figure 5.6.

In Figure 5.6, one can observe the system in terms of the input and the causes and the effects within the system. An input to query the database using the Select(report) triggers the control logic to initiate the execution to generate the report, the execution of which also processes the report generated and initiates a passive effect to print the report. Another pattern that can be observed is in the generation of a ticket. The selection of the lottery game triggers the program control logic to initiate the payment module which on execution issues the ticket and sends it to the printer without prompting the user.

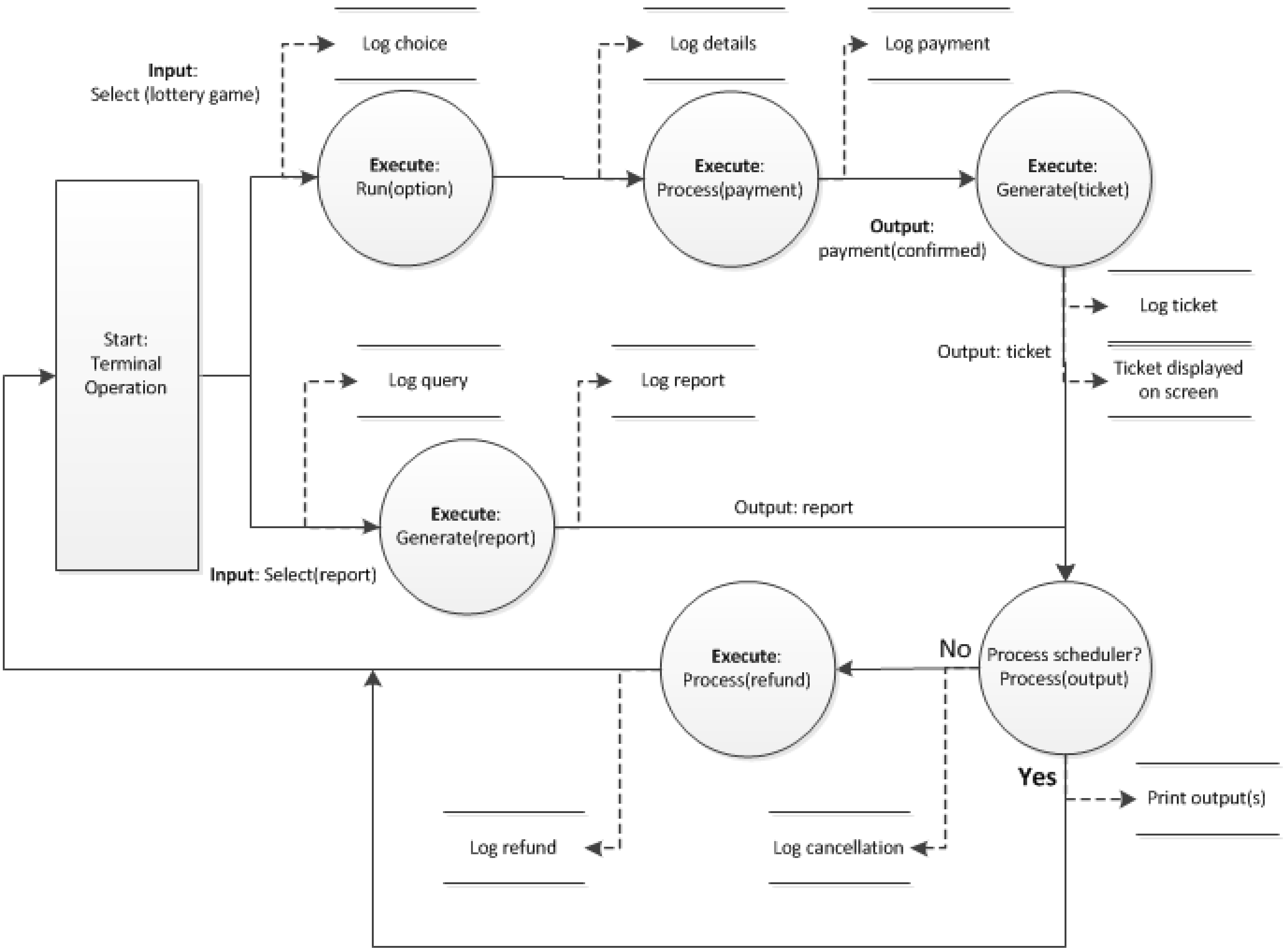


**Figure 5.6:** Cause and Effect pattern (Logic model) of a 5 Cash Game System.

The ticket is also displayed during the process as a passive effect.

To test the hypothesis that the terminal was manipulated, the examiner will then have to determine whether it can be shown that the terminal was manipulated and under what conditions it would be considered necessary and sufficient to demonstrate the manipulation of the terminal and therefore demonstrate the hypothesis to be correct.

The specification of the necessary and sufficient conditions enables an examiner to know what to test. As earlier indicated, the necessary conditions are the conditions without which an event cannot happen while the sufficient conditions are the conditions that guarantee an expected outcome.

The necessary conditions that are required to support the hypothesis that the terminal was manipulated to display the results in a way that would allow the operator an undue advantage in determining the results and enabling the cancellation of unfavourable transactions are articulated as follows. It is necessary to show that

- There were tickets sold within some short time period before the transaction deadline.
- The machine was busy or delayed during the time the winning tickets were printed.
- Only unfavourable tickets during machine busy/delay times were cancelled.

The sufficient condition in this case is expected to provide a definite indicator of malicious activity. It is sufficient to demonstrate the hypothesis holds if it can be shown that:

- The activities specified under the necessary conditions were carried out at numerous times.
- There is a consistent pattern in which these activities happened.

The examiner is required to demonstrate that if there are late sales, and the machine was busy, then tickets sales made were mostly winning tickets and ticket sales cancelled were all unfavourable tickets. Also, the examiner may be able to show that this pattern happened at numerous times in a consistent manner. To test the hypothesis in this way eliminates the chance of having an rival explanation that would take into consideration the necessary and sufficient conditions highlighted in the case. An explanation that cannot explain these conditions of the case is excluded. It is important to note that sufficient conditions may only be found if the hypotheses are narrowed down to a list of possibilities.

The specification of the necessary and sufficient conditions of a case also supports the establishment of a web of consistency. The examiner may, after observing the logs of activities on the system, be able to plot a time series analysis of the case displaying what transactions and at what time they occurred on the system

Examining the logic model in Figure 5.6 further, an analysis of the log of tickets generated provides an examiner with information about whether there were sold tickets within a specified period before the transaction deadline. The result from this query provides the examiner with data for further analysis to demonstrate the necessary requirement which is to determine the tickets that were processed during the time the machine was busy or delayed.

To do this, the results from querying the sold ticket log are compared with the log of reports generated. This analysis is based on the knowledge that the machine will be busy or delayed when the suspected tickets were generated and during the time when the reports were being processed. The result of this analysis provides the examiner with a smaller set of tickets that were generated during the time the machine was busy or delayed. From this result set, an examiner expects to find that winning tickets were printed, and non-winning tickets were cancelled. To determine whether that only unfavourable tickets during machine busy times were cancelled, the result set is then compared with the log of cancelled transactions. From this analysis, an examiner can show that a larger number of unfavourable tickets were cancelled and the remaining tickets which were not cancelled were largely winning tickets.

An examiner has successfully demonstrated the correctness of the hypothesis when the necessary conditions for the case have been tested and not disproved. This indicates that the terminal could have been manipulated in a way that the results could have been known before the transaction was completed and unfavourable transactions were deliberately cancelled. To demonstrate sufficient proof of the hypothesis, an examiner can widen the scope of the examination to other time frames within the same machine to demonstrate that this manipulation was carried out over several times thereby establishing a web of consistency. It may also be sufficient to demonstrate that tickets sold at other times which were non-winning tickets were sold when the machine was not busy and are legitimate transactions carried out on behalf of a lottery user by the retailer.

Using replication logic, an examiner can also expand the scope of the examination into a multiple case examination. By applying literal replication, an examiner can examine several other suspected terminals using the same conditions and sufficiently demonstrate the manipulation was done on these suspected terminals. This further confirms and strengthens the hypothesis and enables a web of consistency to be established. By applying theoretical replication, an examiner can select another set of suspected terminals and examine them to invalidate the hypothesis i.e. to demonstrate that the manipulation cannot be found thereby invalidating the rival hypothesis. Another process of theoretical replication is to select a few known "clean" terminals and show that the kind of manipulation found on the suspected terminals cannot not be found on the "clean" terminals.

The identification, testing and validation of the necessary and sufficient conditions of a hypothesis and the application of analytical techniques and strategies employed in the case study method strengthens an examination though the demonstration of causal relationships and a web of consistency which ensures that the findings of an examination is consistent and reliable.

The analysis of this case employed the use of the logic model technique to illustrate the application of analytical techniques in examination of occurrences in a digital system. Similarly, the application of other analytical techniques such as pattern matching, explanation building, time series analysis and cross-case synthesis can also be applied in establishing findings in digital forensic examinations.

## 5.4 Summary

This chapter set out to demonstrate the practicality of the case study method in examining digital occurrences. The focus was to apply the case study method in establishing the findings of digital forensic examinations. We examined the relationship between digital evidence and its plausible causes and how patterns can be identified and applied in demonstrating findings in a digital forensic evidence examination. By applying Yin's case study method, a forensic examiner can establish relationships that support and validate the findings of a forensic examination.

Chapter 6 discusses the reliability of the findings of a forensic examination. It further explores how the case study method can be applied in validating the findings made in a forensic examination. The suitability and applicability of the method's four validity tests and the tactics applied in satisfying these tests are applied in a digital forensic environment ensure that a logical approach has been followed and that the findings follow from the underlying hypotheses.

# Chapter 6

# A Discussion of the Case Study Model

This chapter focuses on exploring discussion areas on the application of the case study method. The application of case study in policing and laboratory work is explored as well as the reliability and validity of the case study method. The case study model is expected to be applied in a variety of situations. These situations will typically be in digital forensic examinations especially in crime scene investigations by the police and in evidence examination in the laboratory. While it is expected that there are several other examination methods in use by forensic examiners in digital crime investigations, this chapter proposes the case study method as a suitable alternative approach to other methods currently used for digital evidence examinations. The discussions provided in this chapter are divided into two sections.

In section 6.1, the author provides a discussion around applying the case study method in areas such as policing and laboratory work which are the two areas where digital forensic examinations are mainly carried out. In these areas, the discussion explores the suitability of the case study method when applied in investigating digital crimes.

Section 6.2 evaluates the case study method in relation to a United States report [23] on forensic science in criminal courts. This report is geared towards ensuring scientific validity of feature-comparison methods. Feature-comparison methods are generally focused on identification, i.e. determining whether an evidential sample possibly obtained from the crime scene is associated with potential attributive sample possibly obtained from a suspect, based on the presence of similar patterns, impressions, or other features in the evidential sample and the attributive sample. These include methods such as applied in the analysis of DNA, latent fingerprints, hair, toolmarks and bitemarks, firearms and spent ammunition, shoeprints and tyre tracks, and handwriting. The report evaluates these methods applied in forensic science fields with a view to determine where improvements can be made in strengthening the validity of findings in these forensic-science disciplines. While this report is specifically geared towards making improvements in forensic science within the United States legal system, the application of forensic science is generally the same and therefore, the report is relevant in its application to assess forensic science practices in other parts of the world.

The concluding section provides a summary of the chapter.

## 6.1 Application of the Case Study Method in Policing and Laboratory Work

The case study method can be applicable in several different industry areas and as noted in the introductory section of this chapter, the situations where digital forensic examination methods are typically applied are mostly in crime scene investigations conducted by the police and in evidence examination in the laboratory. This section explores both aspects.

In crime scene investigations, the goal of a detective or crime scene investigator is to investigate, to find the evidence that demonstrates a claim. While carrying out an examination, the goal is mainly to analyse evidence to demonstrate its validity and the inferences made from the evidence. The case study method is suitable when applied as an investigative approach and as an approach for examining evidence.

A police investigation or a criminal investigation typically incorporates several activities that cannot be considered as scientific and even those activities that are “scientific” mostly do not have scientific underpinnings. The identification and determination of evidential material is mostly objective and dependent on what is observed in the crime scene. While evidence identification itself cannot be totally considered as scientific, the need to identify relevant evidence in a criminal case cannot be over emphasised. Evidence that is overlooked may either have probative value or may be suitable as exculpatory evidence in a criminal investigation. Police investigators also find that leads that are investigated are very often incorrect and based on evidence that cannot be relied upon. The decision to follow or abandon leads are also found not to be objectively defined nor are these decisions validated by the application of objective criteria. This indicates that the reasoning and approach employed in criminal investigations are often not repeatable nor is the logic that lead to the conclusions and inferences arrived at by police investigators.

What often determines the course and decisions followed in most police investigations is the years of experience the investigator has in solving crimes, the skill and intuition possessed by the investigator, the behaviour of the suspects investigated before and after the crime, the bias of the investigator, the requirement by the law to obtain warrants to search and obtain evidence from the suspects as well as other permissions that may be required.

While it is expected the investigation will often uncover relevant facts that point to a certain conclusion for the investigation, it is often observed that rival explanations are not often taken into consideration or presented as alternative facts that should be considered in a case. The case study method applies several tactics, which can also be considered as principles that when applied in a police investigation can prove to be instrumental in ensuring the conclusions and inferences made in an investigation are based on a reliable and repeatable approach. It has been noted earlier that though the process of evidence identification cannot be considered as scientific, there is a need to identify evidence that is suitable and relevant to the investigation from which analysis and inferences can be made.

Forensic examinations in laboratories provide a more structured approach to analysing evidence. Laboratories often focus on a specific type of analysis or test. As noted in chapter 4, much of what happens in a forensic laboratory reflects what is known in the application of the case study method. Unlike crime scene investigations that focus on the general crime scene, laboratory analysis focuses on answering specific questions that were raised by the investigative team. Investigations are carried out by detectives, and the findings from these investigations are compiled and submitted to the court as evidence. In laboratories, evidence is analysed, and claims are made by scientists about the evidence by applying scientific approaches. This indicates a clear differentiation between the work of detectives and scientists. A scientist tests a hypothesis and returns a result without bias. The result of the hypothesis may not favour the claim the investigator seeks to demonstrate or may even on occasion be found to be inconclusive. The detective on the other hand investigates a crime even while not certain that a crime was committed. The detective plots a course through the crime scene searching for leads, facts, and opinions which most often cannot be tested or validated. The detective may often formulate hypotheses about what happened and more often these hypotheses are not in a form that enables them to be testable and falsifiable. The detective often aims to find as many leads, facts and opinions that make a case suitable for prosecution without the underlying proof of evidence reliability and validity. In this way, the detective is a puzzle solver while the scientist tests theories.

The case study method assists the investigator or detective by focusing the investigation on the questions that need to be answered by the case and enables the investigator to address these questions as problems and then hypotheses that enable the application of science to the investigation. These questions may be a decision problem which addresses the investigation in terms of what needs to be tested and the narrative problem which addresses the investigation in terms of finding root causes. These enable the investigator to focus attention on what evidence is important to the case.

The case study method incorporates three requirements that assist the investigator in making informed decisions about what evidence is relevant to the investigation. The first requirement is that an understanding of the inner workings of the system is required by a forensic examiner in determining the likely sources of evidence and where these sources of evidence are located.

The second requirement is to use multiple evidence sources where possible which enables an investigator to demonstrate the reliability of the plausible evidence sources. The third requirement expects the investigator to address rival explanations. This is instructive in that while collecting evidence, the investigator is required to also collect and analyse evidence that may be contradictory to what the investigator intends to demonstrate. This enables the investigator to refute rival explanations and by invalidating rival explanations, reinforce the reliability of the findings and inferences made in the investigation. The case study approach provides a crime scene investigator with a logically thought-out approach to reaching a conclusion that is reproducible, testable and falsifiable. In this way, the case study method can be applied as an investigative method of inquiry that supports the investigative process.

## 6.2 Evaluating the Reliability and Validity of Case Study Method

In September 2016, a report was released by the United States presidential committee, the President's Council of Advisors on Science and Technology (PCAST) titled: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods [23]. This report was mandated to determine whether additional steps could be taken to strengthen forensic science disciplines and ensure that forensic evidence produced in the court was valid. PCAST focused on forensic science disciplines that apply feature-comparison methods in examining evidential data. Feature-comparison methods attempt to determine whether evidence obtained from a crime scene is comparable with evidence obtained from a potential suspect. The report focused mainly on methods applied in analysis of DNA, hair, latent firearms and spent ammunition, toolmarks and bitemarks, shoeprints and tyre tracks, and handwriting.

Due to developments in the past two decades where forensic science has played a crucial role in the determination of a case by the courts, some of these cases including wrongful convictions, increasing attention has been focused on the question of the scientific validity and reliability of some important forms of forensic evidence and of testimony based upon them. PCAST concluded two important gaps requiring the committee's attention:

> *the need for clarity about the scientific standards for the validity and reliability of forensic methods*, and
>
> *the need to evaluate specific forensic methods to determine whether they have been*

> *scientifically established to be valid and reliable.*

The study aimed to determine how the gaps in several forensic science disciplines particularly "feature-comparison" methods can be closed to strengthen scientific validity of the methods applied in forensic science disciplines. In this section, a review of the aspects of the study covering the criteria and evaluation of several forensic science disciplines are discussed. Furthermore, the criteria are then applied to evaluate the case study method and determine its validity as a forensic science method for digital evidence.

The PCAST report focused on two types of scientific validity in evaluating a forensic science method: "foundational validity" and "validity as applied". Foundational validity focuses on the reliability of the method and its suitability for application to the intended problem. It requires that a forensic science method is demonstrated empirically to be repeatable, reproducible, and accurate at the level of its measurement, and be suitable for application to the field in which it is applied. Validity as applied on the other hand, focuses on the application of the method in practice to forensic cases. It requires that the method has been reliably applied in practice.

In evaluating foundational validity and validity in practice of forensic science disciplines, PCAST noted that scientific methods may depend either on objective or subjective applications based on the design of the methods. Objective applications require limited human judgement in interpretation of the findings of the method eliminating issues of human error and cognitive bias. However, a forensic method which is subjective relies heavily on human judgement and is vulnerable to human error, inconsistencies in reproducibility among examiners, and cognitive bias. To critically assess forensics science methods whether objective or subjective, PCAST provided a set of criteria to satisfy foundational validity and validity as applied.

For foundational validity, it is required that:

- the method has been subjected to empirical testing by multiple groups under the conditions in which it is intended for use and the method is demonstrated to be repeatable and reproducible, and that the method is able to provide valid estimates of its accuracy.

- for objective methods, measuring the accuracy, reproducibility and consistency of each individual step in the method validates the method's foundational validity.

- for subjective feature-comparison methods, the method is suitably evaluated for validity and reliability in its entirety as a black-box study involving many independent tests using "known" and "questioned" samples to determine the error rates.
- without providing an appropriate estimate of accuracy, an examiner's conclusion that two samples are similar or indistinguishable is considered baseless.

For validity as applied, it is required that:

- the forensic examiner's capability to demonstrate the reliable application of the method must have been shown by ensuring the documentation i.e. procedures, findings, processes are available to other scientists for review.
- the forensic examiner must demonstrate scientifically any assertions or inferences made about the probative value of the evidence. The forensic examiner should report the method's overall error rates and demonstrate that the evidential samples examined are relevant to the facts of the case and inferences made are empirical and are valid inferences inferred from the evidence within the context of the case.

As noted above, the PCAST study focused mainly on methods applied in analysis of DNA, hair, latent firearms and spent ammunition, toolmarks and bitemarks, shoeprints and tyre tracks, and handwriting and while the findings from this report are important, the goal of this section is to assess the criteria in relation to examinations in digital forensics using the case study approach.

The PCAST criteria for foundational validity require that the method be repeatable and reproducible. The case study method applies a defined analytical set of practices in examining digital evidence. The application of defined logical patterns and analytical strategies, techniques and tactics defined in the case study method by a forensic examiner ensures that findings are obtained from well-structured logical practices that are repeatable, and reproducible. The case study method using this set of practices assists the forensic examiner in validating the findings of the study. For example, applying the logic of literal replication enables a forensic examiner to validate a hypothesis using a similar case to strengthen the findings of the case. The logic of theoretical replication enables the forensic examiner to test rival explanations or theories under the same conditions as the main explanation to invalidate them.

The case study method itself also provides for the validation of the design of the digital forensic examination as a case study. The validity test that focuses on the repeatability and reproducibility of the case is the test for internal validity. As discussed in chapter 4 of this research, internal validity tests the logic that led to the findings of the study to confirm that the findings reflect what was analysed. It critiques the forensic examiner's findings and asks the question "how are we sure that our findings reflect the outcome of the case and that there are no other factors that may have influenced our findings?" Within the case study method, four tactics can be applied in strengthening internal validity. These tactics are pattern matching, explanation building, addressing rival explanations and logic models.

In addressing internal validity within the case study method and also to satisfy the criteria for foundational validity, the pattern matching tactic compares patterns based on the findings of the empirical case study with the predicted pattern(s) or hypothesis made, with the goal of showing that the matching of predictions made before empirical observation provide a stronger argument for the validity of the study. In other words, a forensic examiner can infer from the input to the system and the system configuration, the expected traces that can be observed within the system. Observing these traces provides proof of valid application of logical patterns implemented within the system. An explanation building tactic is applied to analyse the evidence to build an explanation about the case by establishing the relationships between the variables or conditions of the case. This technique enables the forensic examiner to account for all the conditions that produced the evidence and showing that all the pieces fit into the case. The development of rival explanations or theoretical propositions as a tactic for assessing internal validity is considered a very reliable tactic in validating a case study design. The tactic enables a forensic examiner to develop the hypotheses of the case in a way that plausible rival explanations of the case are mutually exclusive, that is, if one explanation is valid, the other cannot be valid. In this way, the forensic examiner can apply the logic of replication; literal replication or theoretical replication in demonstrating the claims made. Logic models as a tactic breaks down a complex chain of events into repeated cause-effect patterns to reflect intermediate findings and final findings within a case. By reconstructing the sequence of events that caused the evidence, a forensic examiner can demonstrate that the case is reproducible and repeatable and demonstrate that there are no missing pieces in the case that are not accounted for within the explanation presented from the findings of the case. These tactics employed in the case study method demonstrate repeatability and reproducibility which satisfies the criteria for foundational validity.

The second PCAST criteria covers the scientific criteria for validity as applied. These criteria focus mainly on the reliability and error rates of the method. The case study method does not directly address the error rates of the method but provides validity tests that ensure the method has been adequately applied. These tests include construct validity, internal validity and reliability tests. The tests for internal validity have been discussed when addressing the PCAST foundational validity test. Therefore, the focus will be on construct validity and reliability tests.

The test for construct validity justifies the evidence collection process. It tests the rationale behind the examiner's decision on what evidence to collect. This is to ensure that given any forensic question relating to the case, the forensic examiner can demonstrate that sufficient digital evidence was collected to answer the question asked of the evidence. The method employs three tactics or actionable principles in satisfying the requirement for construct validity: the use of multiple sources of evidence consistent with Casey's certainty scale, establishing a chain of evidence or chain of custody, and peer reviewing the study findings.

The case study method also employs the test for reliability. Reliability in a digital forensic examination is crucial to ensure that the findings are consistent, and a structured approach was followed within the examination. The tactics employed by the case study method in satisfying the test for reliability is to provide full documentation of evidence, processes as well as the actions taken throughout the examination. Documentation of all steps taken throughout the life cycle of the digital evidence examination ensures repeatability and reliability of the examination process and demonstrates that a structured approach was followed in carrying out the digital forensic examination. We note that while the case study method does not enable a forensic examiner to quantify and report error rates, its tests for validity and associated tactics enable a forensic examiner to qualitatively demonstrate, using the method validity tests and associated tactics, that the method is scientifically valid and has been reliably applied to produce consistent and reliable findings from a digital forensic examination.

## 6.3 Summary

This chapter explored various topics relating to the application of the case study method in areas of crime scene investigation and in laboratory work. The case study method was shown to be suitably applied in these areas. Furthermore, the reliability of the case study method was evaluated using the PCAST criteria. While the case study method does not completely satisfy the quantitative requirement for validity as applied criterion in the determination of the method's error rates, the method applies tactics in ensuring the validity of the method by applying tests for construct validity and reliability and employing tactics inherent in the method in satisfying the requirement for the method's reliability

The next chapter provides a conclusion for the work done in this research and summarises the conclusions and future work for which this research can provide a basis.

# Chapter 7

# Conclusion

This research work examined case study research as a method for digital forensic examinations. The underlying work examines whether case study research is a suitable scientific foundation for digital forensic examinations. It was demonstrated in the research, that the method can be suitably applied in determining and establishing causes and validating the findings of a digital examination.

The impact of this research on the forensic science community is two-fold. The first is to propose an alternative methodical approach for digital examinations which can be applied where experiments are not possible. The second is to explore and propose strategies for examining and validating the findings of digital forensic examinations.

In forensic examinations, one of the key questions involves the reliability of the findings of a forensic examination. Also, the challenge of this research was primarily one of mapping the case study method suited to the social sciences to digital forensics which is primarily in the natural sciences. To reflect on the suitability of the case study method, the literature was mapped to analytical strategies and techniques employed in digital forensic examinations. The techniques that make case study a suitable method in research also applied in digital forensic examinations.

Based on the application of the case study approach applied in forensic examinations, the conclusion of this research is that the author's adaptation of Yin's case study method or a suitable adapted method of case study research, would be applicable to digital forensic examinations.

The research further explored approaches to carrying out a digital examination, the strategies to establishing inferences when examining evidence and justifying claims made in an examination for the purposes of conducting a proper evidence examination and demonstrating a logical reconstruction of the facts or findings derived from the examination of the case.

In reviewing the work done in this research, the method explored answers to two main forms of questions. The first form addresses a decision problem, where the outcome is often determined by empirical evidence derived by measurement and observation. The second form addresses a narrative problem where the outcome is determined by analytical techniques and tactics applied in an in-depth examination of the case. These forms of questions provide the basis for a digital examination and are applied in the formulation of hypotheses. The main hypothesis and plausible rival hypothesis reflect what will be proved or falsified in an examination.

Inherent in the method is a methodical approach to conducting a digital examination. This is the design of the case study. Hypotheses are formulated by a forensic examiner based on the questions that need to be answered. The main hypothesis reflects what the examiner expects to observe and demonstrate within the context of the case. Rival hypotheses are plausible explanations that oppose the main hypothesis and are required to be disproved. Depending on the complexity of the case, the method is suitably applied in isolated cases or multiple case studies involving dispersed events.

In examining the evidence, the application of analytical strategies and techniques establish a web of consistency within the evidence and demonstrate its reliability. The rationale behind establishing a web of consistency is one of utmost importance to the method. The more tightly coupled the patterns found during evidence analysis, the less likely there will be plausible rival explanations that can readily explain all the facts of the case. The concept of establishing a web of consistency proposed in this research is considered a contribution to the forensic science body of knowledge.

Using any of four analytic strategies (relying on the case hypotheses, working the data from ground up, developing a case description, examining plausible rival explanations), analytical techniques which include pattern matching, explanation building, time-series analysis and logic models are applied to demonstrate webs of consistency.

Pattern matching is applied mainly when the strategy relies on the case study hypothesis. It compares patterns based on the findings with the predicted pattern made before the evidence was analysed. Explanation building is applied when working to case from the ground up. Time-series analysis is applied in tracing the changes in the state of a phenomenon over time. Logic models are a form of pattern matching and are applied to break down complex events into repeated cause and effect patterns to reflect how the conclusions were reached from intermediate findings.

The question of the validity of the findings of a forensic examination was also examined. This involves three tests which are construct validity, internal validity and reliability. In satisfying these tests, tactics are applied. The test for construct validity critiques the justification for the evidence collected for examination. The test for internal validity critiques the findings of a study. The test for reliability critiques the reproducibility of the examination. These tests ensure that the findings are consistent, and a structured approach was followed in carrying out the digital examination.

The method's three validity tests (construct validity, internal validity and reliability) further address the requirement for reliability. Construct validity justifies the evidence collected for examination, internal validity justifies the findings and reliability test demonstrates the examination reproducibility. Tactics applied to satisfy these tests ensure that the findings follow from the underlying hypotheses and are peer reviewed. The examination is also repeatable and rival explanations are refuted strengthening the examination findings.

Causality is a crucial element in this research and particularly in evidence analysis and attribution. This research demonstrates the notion of causality in digital systems by exploring the establishment of causal relationships in evidence analysis. The specification of the necessary and sufficient conditions for causality, establishing of a web of consistency within evidence and refutation of plausible rival explanations are central to establishing causal relationships.

In applying causality to digital systems, the notion of causality is extended by formalising the notion of causality in its forward motion and backward motion. The context of a digital system which is controlled by the control logic is held in this research. The control logic is the cause in a digital system and requires an input, the execution of which may cause an effect within the system. This effect may be active in the form of program executions or passive in the form of traces. The notion of causality in its forward motion enables a forensic examiner to define a view of a digital system based on its expected mode of execution or behaviour. This enables a forensic examiner to identify and examine plausible causes and validate traces thereby reconstructing the events observed in the case. The notion of causality in its backward motion defines a view of the digital system based on the traces observed. From the traces found in a system, a forensic examiner can predict the system configuration and input to the system at the time and attempt a complete reconstruction of the events of the case applying the strategies and techniques inherent in the case study method.

## 7.1 Future Work

This research work explored the application of the case study method in digital forensics examination and while the suitability of the method in digital forensic science has been established, further research into the application of the case study method in several digital forensic cases are necessary to reinforce the method's applicability to the field of digital forensic science. In addition, the method is inherently limited due to its origin in the social science field by its qualitative approach to reliability and error rate. While the method incorporates strategies and tactics applied in validating the findings of the examination, further research is needed to explore the suitability of qualitative techniques applied by the method in the field of digital forensic examinations.

# Bibliography

[1] Susan Ballou. *Electronic crime scene investigation: A guide for first responders.* Diane Publishing, 2010.

[2] David E Bernstein. Junk science in the United States and the Commonwealth. *Yale J. Int'l L.*, 21:123, 1996.

[3] Mario Bunge. *Philosophy of science: from problem to theory*, volume 1. Transaction Publishers, 1998.

[4] Brian Carrier. Open source digital forensics tools: The legal argument. Technical report, stake, 2002.

[5] Brian Carrier. Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of digital evidence*, 1(4):1–12, 2003.

[6] Brian D Carrier. *A hypothesis-based approach to digital forensic investigations.* ProQuest, 2006.

[7] Eoghan Casey. *Handbook of digital forensics and investigation.* Academic Press, 2009.

[8] Eoghan Casey. *Digital evidence and computer crime: Forensic science, computers, and the internet.* Academic press, 2011.

[9] Fred Cohen. *Challenges to digital forensic evidence.* Fred Cohen and Associates, 2008.

[10] Frederick B Cohen. *Digital forensic evidence examination.* Asp Press, 2009.

[11] Frederick B Cohen. Fundamentals of digital forensic evidence. In *Handbook of Information and Communication Security*, pages 789–808. Springer, 2010.

[12] Supreme Court. Daubert v. Merrell Dow Pharmaceuticals, Inc. https://supreme.justia.com/cases/federal/us/509/579/case.html, 1993. Accessed: 2017-07-16.

[13] Dist. of Columbia Court of Appeals. Frye v. United States. https://www.law.ufl.edu/_pdf/faculty/little/topic8.pdf, 1923. Accessed: 2017-07-16.

[14] Margaret G Farrell. Daubert v. Merrell Dow Pharmaceuticals, Inc.: Epistemilogy and Legal Process. *Cardozo L. Rev.*, 15:2183, 1993.

[15] Herbert Feigl. The origin and spirit of logical positivism. In *Inquiries and Provocations*, pages 21–37. Springer, 1981.

[16] Simson Garfinkel, Paul Farrell, Vassil Roussev, and George Dinolt. Bringing science to digital forensics with standardized forensic corpora. *digital investigation*, 6:S2–S11, 2009.

[17] Paul C Giannelli. The admissibility of novel scientific evidence: Frye v. United States, a half-century later. *Columbia Law Review*, 80(6):1197–1250, 1980.

[18] Pavel Gladyshev. *Formalising event reconstruction in digital investigations*. PhD thesis, University College Dublin, 2004.

[19] Pavel Gladyshev and Ahmed Patel. Finite state machine approach to digital event reconstruction. *Digital Investigation*, 1(2):130–149, 2004.

[20] Pavel Gladyshev and Ahmed Patel. Formalising event time bounding in digital investigations. *International Journal of Digital Evidence*, 4(2):1–14, 2005.

[21] CP Grobler, CP Louwrens, and Sebastiaan H von Solms. A multi-component view of digital forensics. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, pages 647–652. IEEE, 2010.

[22] Sven Ove Hansson. Science and pseudo-science. *Stanford Encyclopedia of Philosophy, Stanford*, 2008.

[23] J Holdren and E Lender. Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods. *Subcommittee on the Social and Behavioral Sciences Team: United States Government*, 2016.

[24] Keith Inman and Norah Rudin. *Principles and practice of criminalistics: the profession of forensic science*. CRC Press, 2000.

[25] LII / Legal Information Institute. Rule 702. Testimony by Expert Witnesses. https://www.law.cornell.edu/rules/fre/rule_702. Accessed: 2017-07-16.

[26] Thomas S Kuhn. BOOK AND FILM REVIEWS: Revolutionary View of the History of Science: The Structure of Scientific Revolutions. *The Physics Teacher*, 8(2):96–98, 1970.

[27] Thomas S Kuhn. *The structure of scientific revolutions*. University of Chicago press, 2012.

[28] Larry Laudan. The demise of the demarcation problem. *Physics, philosophy and psychoanalysis*, pages 111–127, 1983.

[29] Jason T Luttgens, Matthew Pepe, and Kevin Mandia. *Incident response & computer forensics*. McGraw-Hill Education Group, 2014.

[30] J Todd McDonald, Yong C Kim, and Alec Yasinsac. Software issues in digital forensics. *ACM SIGOPS Operating Systems Review*, 42(3):29–40, 2008.

[31] Justin J. McShane. The Locard Exchange Principle In Forensic Science: The Real Itouch. http://www.thetruthaboutforensicscience.com/the-locard-exchange-principle-in-forensic-science-the-real-itouch/, 2010. Accessed: 2015-06-12.

[32] Mdlottery.com. Maryland Lottery - Games 5 Card Cash. https://http://www.mdlottery.com/games/5-card-cash/, 2016. Accessed: 2016-04-27.

[33] Peter Morales. Science and the Search for Meaning. *The New Atlantis*, 2013.

[34] Bill Nelson, Amelia Phillips, and Christopher Steuart. *Guide to computer forensics and investigations*. Cengage Learning, 2014.

[35] National Institute of Justice. NIJ's Forensic Science Research and Development Portfolio. https://www.nij.gov/topics/forensics/Pages/welcome.aspx#randd. Accessed: 2017-07-16.

[36] National Institute of Justice and National Research Council. *Strengthening Forensic Science in the United States: A Path Forward*. National Academies Press, Washington, DC, 2009.

[37] Organization of Scientific Area Committees. Scientific Area Committees. https://www.nist.gov/topics/forensic-science/osac-organizational-structure. Accessed: 2017-11-25.

[38] Martin S Olivier. On metadata context in database forensics. *Digital Investigation*, 5(3):115–123, 2009.

[39] Martin S Olivier. On complex crimes and digital forensics. *Information Security in Diverse Computing Environments*, pages 230–244, 2013.

[40] Martin S Olivier. Towards a digital forensic science. In *Information Security for South Africa (ISSA), 2015*, pages 1–8. IEEE, 2015.

[41] Martin S Olivier. On a scientific digital forensic theory. In Gilbert Peterson and Sujeet Shenoi, editors, *Advances in Digital Forensics XII*, IFIP Advances in Information and Communication Technology — Advances in Digital Forensics. Springer, 2016.

[42] Martin S Olivier and Stefan Gruner. On the Scientific Maturity of Digital Forensics Research. In Gilbert Peterson and Sujeet Shenoi, editors, *Advances in Digital Forensics IX*, IFIP Advances in Information and Communication Technology — Advances in Digital Forensics, pages 33–49. Springer, 2013.

[43] Oluwasayo Oyelami and Martin Olivier. Establishing Findings in Digital Forensic Examinations: A Case Study Method. In *IFIP International Conference on Digital Forensics*, pages 3–21. Springer, 2017.

[44] Oluwasayo Oyelami and Martin S Olivier. Using Yin's Approach to Case Studies as a Paradigm for Conducting Examinations. In Gilbert Peterson and Sujeet Shenoi, editors, *Advances in Digital Forensics XI*, volume 462 of *IFIP Advances in Information and Communication Technology*, pages 45–59. Springer, 2015.

[45] Gary Palmer. A Road Map for Digital Forensic Research: Report from the First Digital Forensic Research Workshop (DFRWS). *Utica, New York*, 2001.

[46] Mark Pollitt. Digital Forensics as a Surreal Narrative. In *Advances in Digital Forensics V*, pages 3–15. Springer, 2009.

[47] Mark Pollitt. History, historiography and the hermeneutics of the hard drive. In *Advances in Digital Forensics IX*, pages 3–17. Springer, 2013.

[48] Karl Popper. Philosophy of science. *British Philosophy in the Mid-Century (ed. CA Mace). London: George Allen and Unwin*, 1957.

[49] Karl R Popper. The problem of demarcation. *Philosophy: Basic Readings*, pages 247–57, 1999.

[50] Lottery Post. Six now face charges in ct lottery scheme. https://www.lotterypost.com/news/301512, 2016. Accessed: 2016-04-27.

[51] Innocence Project. Innocence Project. https://www.innocenceproject.org/cases/. Accessed: 2017-07-16.

[52] David B Resnik. A pragmatic approach to the demarcation problem. *Studies in History and Philosophy of Science Part A*, 31(2):249–267, 2000.

[53] Friedrich Stadler. *The Vienna circle: studies in the origins, development, and influence of logical empiricism*, volume 4. Springer, 2015.

[54] Segen Tewelde, Martin S Olivier, and Stefan Gruner. Notions of Hypothesis" in Digital Forensics. In Gilbert Peterson and Sujeet Shenoi, editors, *Advances in Digital Forensics XI*, volume 462 of *IFIP Advances in Information and Communication Technology*, pages 29–43. Springer, 2015.

[55] Aleksandar Valjarevic and Hein S Venter. Implementation guidelines for a harmonised digital forensic investigation readiness process model. In *Information Security for South Africa, 2013*, pages 1–9. IEEE, 2013.

[56] Aleksandar Valjarevic and Hein S Venter. A comprehensive and harmonized digital forensic investigation process model. *Journal of forensic sciences*, 60(6):1467–1483, 2015.

[57] R.L.K. Virchow. *Post-Mortem Examinations.* Theclassics Us, 2013.

[58] Carrie Morgan Whitcomb. An historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, 1(1):7–15, 2002.

[59] CM Whitcomb. The Evolution of Digital Evidence in Forensic Science Laboratories. *The Police Chief, 74 (11)*, 2007.

[60] Jack Wiles and Anthony Reyes. *The best damn cybercrime and digital forensics book period.* Syngress, 2011.

[61] Sue Wilkinson and D Haagman. Good practice guide for computer-based electronic evidence. *Association of Chief Police Officers*, 2010.

[62] Svein Willassen. Hypothesis-based investigation of digital timestamps. In *Advances in Digital Forensics IV*, pages 75–86. Springer, 2008.

[63] Ludwig Wittgenstein et al. Wittgenstein and the Vienna Circle: Conversations recorded by Friedrich Waismann. *Ed. Brian McGuinness. Trans. Joachim Schulte and Brian McGuinness. Oxford: Basil Blackwell*, 1979.

[64] Robert K Yin. *Applications of case study research.* Sage, 2011.

[65] Robert K Yin. *Case study research: Design and methods.* Sage publications, 2013.

[66] Robert K Yin. *Case study research and applications: Design and methods.* Sage publications, 2017.

[67] Edward N Zalta, Uri Nodelman, and Colin Allen. Stanford encyclopedia of philosophy, 2003.

[68] K Zantyko. Commentary: Defining digital forensics. *Forensic Magazine*, 20, 2007.

# Appendix A

# Derived Publications

The following list includes a list of the publications derived from this dissertation.

- Oluwasayo Oyelami and Martin S Olivier. Using Yin's approach to case studies as a paradigm for conducting examinations. In Gilbert Peterson and Sujeet Shenoi, editors, Advances in Digital Forensics XI, volume 462 of IFIP Advances in Information and Communication Technology, pages 45-59. Springer, 2015.
- Oluwasayo Oyelami and Martin S Olivier. Establishing Findings in Digital Forensic Examinations - A Case Study Method. In Gilbert Peterson and Sujeet Shenoi, editors, Advances in Digital Forensics XIII, volume 511 of IFIP Advances in Information and Communication Technology, pages 3-21. Springer, 2017.