THE USE OF ELECTRONIC EVIDENCE IN FORENSIC INVESTIGATION

by

AMANDA REFILOE NGOMANE

submitted in accordance with the requirements for
the degree of

MAGISTER TECHNOLOGIAE

in the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: J S HORNE

CO SUPERVISOR: M E VAN ZYL

JUNE 2010

DECLARATION

Student number: 3631-5257

I, Adv. Amanda Refiloe Ngomane, hereby declare that this dissertation entitled:
"The use of electronic evidence in forensic investigation" for a Masters Degree was researched, compiled and drafted by myself and is indeed my own work.

_____

Adv. Amanda Refiloe Ngomane

Signed at Pretoria, South Africa, June 2010

ACKNOWLEDGEMENTS

I would like to convey my profound gratitude to my supervisor Juanida Horne and my mentor and co-supervisor, Marielize Van Zyl, for their considerate guidance, kind supervision, invaluable advice, persistent support and encouragement throughout my study.

I would also like to convey my heartiest gratitude and respect to all the expert participants for their kind gesture and invaluable suggestions and my thanks also goes to all my colleagues for their kind cooperation and for making it possible for me to complete this study.

Finally, I express my gratitude to my family for their support and perseverance.

ABSTRACT

For millions of people worldwide the use of computers has become a central part of life. Criminals are exploiting these technological advances for illegal activities. This growth of technology has therefore produced a completely new source of evidence referred to as 'electronic evidence'. In light of this the researcher focused on the collection of electronic evidence and its admissibility at trial. The study intends to assist and give guidance to investigators to collect electronic evidence properly and legally and ensure that it is admitted as evidence in court. Electronic evidence is fragile and volatile by nature and therefore requires the investigator always to exercise reasonable care during its collection, preservation and analysis to protect its identity and integrity. The legal requirements that the collected electronic evidence must satisfy for it to be admissible in court are relevance, reliability, and authenticity.

When presenting the evidence in court the investigator should always keep in mind that the judges are not specialists in the computing environment and that therefore the investigator must be able to explain how the chain of custody was maintained during the collection, preservation and analysis of electronic evidence. The complex technology behind electronic evidence must be clearly explained so that the court is able to understand the evidence in a way that an ordinary person or those who have never used a computer before can. This is because the court always relies on the expertise of the investigator to understand electronic evidence and make a ruling on matters related to it.

Key Terms:
Forensic investigation, Investigation, Evidence, Document, Admissibility.

LIST OF ABBREVIATIONS

ACPO:	Association of Chief Police Offices
IHCFC:	International Hi-Tech Crime and Forensics Conference
INTERPOL:	International Criminal Police Organisation
IOCE:	International Organization on Computer Evidence
NIA:	National Intelligence Agency
SANDF:	South African Defence Force
SAPS:	South African police Service
SAPSFSL:	South African Police Service Forensic Science Laboratory
SARS:	South African Revenue Service
SASS:	South African Secret Service
SWGDE:	Scientific Working Group on Digital Evidence
UCT:	University of Cape Town
UNISA:	University of South Africa
US:	United States

CONFIRMATION OF LANGUAGE EDITING

I, Susan van Tonder, MA Linguistics, ID 6009160072083, hereby declare that I have edited the master's dissertation 'The Use of Electronic Evidence in Forensic Investigation' by Amanda Refiloe Ngomane.

Susan van Tonder
7 June 2010

TABLE OF CONTENTS

CHAPTER 1
GENERAL ORIENTATION

1.1 Introduction

The first concrete step in a scientific research process is to formulate the specific problem to be examined clearly (Welman & Kruger, 2002:11). A literature review conducted by the researcher on electronic forensics revealed that as technology is advancing many people are exploiting these technological advances for illegal activities. A problem for the investigation of these illegal activities is that rarely do law enforcement officials fully recognise the potential for technological evidence to help solve crimes and prosecute criminals. According to Galves and Galves (2004:2), it appears that the culture of law enforcement is inclined to be more focused on the collection and inspection of non-technological evidence. The reason that investigators focus on traditional physical and/or document-based evidence, as explained by Craiger and Shenoi (2007:49), is that they have limited knowledge of and sometimes lack resources to deal with electronic evidence.

The researcher concurs with the views of Galves and Galves (2004:2) that, internationally, criminals integrate technology into their range of crimes but that in their respective roles of upholding justice, investigators, prosecutors, and even judges do not always develop their knowledge of technology, especially with respect to courtroom evidence. As a result of inadequate education, training and awareness, law enforcement agents are unwilling to compromise cases by attempting processes, and the judiciary unwilling to try out procedures, with which they are unfamiliar, as pointed out by Craiger and Shenoi (2007:50).

Galves and Galves (2004:3) reveal that digital technology has facilitated the commission of crimes by criminals who previously may have found that committing crimes the old-fashioned way, such as by robbing, involved a great deal of risk or effort. Chisum and Turvey (2000:11) indicate that the Locard principle states that if two objects touch each other every contact leaves a trail. This means that incriminating information, which includes potential electronic evidence, is always left behind by even the most advanced criminals, including everyone using an electronic device for any kind of activity. This electronic or audit trail, as mentioned by Galves and Galves (2004:2), can be used to

present influential legal evidence against a suspected criminal. According to these authors, this is because the electronic trail exposes an exceptionally probative "digital fingerprint" that can potentially be used to prove a criminal conduct in a court of law.

The researcher's experience in crime investigations suggests that few investigators are well-versed in the evidentiary, technical, and legal issues related to forensic electronic evidence, such as uncovering evidence without compromising its integrity or credibility and the standard or requirements for admitting electronic evidence at a trial. In general, investigators at the Department of Home Affairs in South Africa are not trained in computer crime investigations. Casey (2004:13) points out that electronic evidence is often overlooked, or collected incorrectly, and analysed ineffectively. As mentioned by Craiger and Shenoi (2007:49), this therefore suggests that there is a possibility that valuable evidence is overlooked by law enforcement, which may result in dropped or reduced charges as well as wrongful convictions.

From experience gained by the researcher in the past nine years of crime investigations with the Directorate of Special Operations (Scorpions) and her current employment as a Director of Investigations at the Department of Home Affairs, the researcher shares the same sentiments as Vacca (2005:4), who believes that there should be great research emphasis placed on the computer forensic field of study, coupled with adequate training of the professionals involved in this field. This research is needed to put in place procedures and best practices to uncover electronic evidence without compromising its evidential value at trial.

This research looks at the significance of collecting electronic evidence properly and legally because the courts adhere to high standards of proof when it comes to presenting evidence in court. This will be started by looking at the methodology used in gathering and analysing the data collected in this research. The concept 'electronic evidence' will be defined whereafter the researcher will explore how electronic evidence can be collected without compromising its integrity or credibility at trial. In the final analysis the legal requirements for admissibility of electronic evidence will be unpacked.

1.2 Aims of the research

When undertaking research the researcher should feel confident about answering 'yes' to the question: Will the research build upon existing knowledge about the topic? (Denscombe, 2003:5).

The principal aim of this research is to educate students and professionals in the law enforcement, cyber forensic, computer security, and legal communities and to build upon existing knowledge on electronic evidence and computer crime. The other aims of this research are to:

- Determine what forensic investigation is;
- Determine what electronic evidence is;
- Determine how electronic evidence can be collected without compromising its integrity or credibility at trial; and
- Identify the legal requirements for admitting electronic evidence at a trial.

The research concludes by making certain recommendations on the basis of the findings of the research that can be used to improve cyber crime investigations.

1.3 Purpose of the research

The main drive behind a piece of research is the desire to solve a practical problem and to improve procedures (Denscombe, 2002:27).

The purpose of this research is:

- To evaluate the existing procedures followed by investigators in mining evidence from technology. This is to establish the value of the existing procedures, in an attempt to determine their strengths and weaknesses (Denscombe, 2002:27);
- To explore international practice used to uncover digital evidence. The researcher attempts to break into new territory, to explore literature and existing practice, furthermore to report back on the findings (Denscombe, 2002:27), regarding admissibility of electronic forensic evidence at trial;
- To arrive at recommendations for good practices, based on the results of the data analysis, that address the problem and enhance investigation skills of investigators, if applied (Denscombe, 2002:27); and

- To empower investigators. The researcher hopes that training materials will be developed to assist in empowering and improving skills of investigators (Denscombe, 2002:27).

1.4 Research questions under investigation

Research questions should allow the researcher to provide a succinct, clear and unambiguous response to the inevitable question: 'so what is it exactly that you are doing?' (Holland & Campbell, 2005:35). In light of this and the background information already provided, the following specific research questions need to be answered:

- What is forensic investigation?
- What is electronic evidence?
- How can electronic evidence be collected without compromising its integrity or credibility at trial?
- What are the legal requirements for admissibility of electronic evidence?

1.5 Key theoretical concepts

According to Williams (2000:518), it is important to remember that definitions are not true or false irrespective of the direction a study or social enquiry takes. The following concepts are defined to prevent any misunderstanding.

1.5.1 Forensic investigation

The term 'forensic' by itself refers to courts of law, juristic or court directed and the application of science to answer questions arising from crime or litigation. Forensic investigation is usually associated with the investigation of computer-related crimes, which include corruption, fraud, embezzlement and other white collar crimes (Van Rooyen, 2004:7).

1.5.2 Investigation

Investigation is the systematic search for the truth with the primary purpose of finding a positive solution to a crime with the help of objective or subjective clues (Van der Westhuizen, 1996:01).

1.5.3 Evidence

Evidence is defined as the means of proving or disproving facts in dispute. It comprises all the information and material submitted to a court by the parties concerned to enable the presiding officer to judge and settle a dispute (Joubert, 2001:331).

1.5.4 Document

According to section 221 of the Criminal Procedure Act 51 of 1977, a document includes any record or transcribed computer printout produced by any mechanism or electronic device and any device by which information is recorded, processed, transmitted or stored (South Africa, 1977: sec. 221)

1.5.5 Admissibility

'Admissibility' refers to evidence that is material and relevant. "Material evidence tends to prove facts that are part of an issue, relevant evidence tends to prove the truth of a fact at issue" (McMahon, 2001:140).

1.6 Value of the research

According to Welman and Kruger (2002:256), value entails demonstrating a measure of research competence or problem-solving ability and, to a lesser degree, adding to the body of knowledge in a field of science.

The following associations or establishments and persons can gain from taking into consideration and putting into practice the recommendations emanating from this research:

- UNISA – the findings can be used by researchers and students for referral purposes. They can also be incorporated into curriculum development.
- South African society – the findings can be used to help the South African public to understand the scope of the use of electronic evidence and challenges which investigators are faced with. In addition if the investigators are better skilled they will be able to conduct investigations competently, which in turn will help reduce crime and contribute to a safer society.
- Industry – the South African law enforcement industry with investigative capabilities can use the information for future training to cultivate more professional and improved investigative skills.

1.7 Research design and approach

A research design is an exposition or plan of the way in which the researcher intends to deal with the research problem that has been formulated (Mouton, 1996:175). The reason that a research design is applied to a research study is that it provides the overall structure for the procedures that the researcher follows, the data that the researcher collects and the data analysis that the researcher conducts (Leedy & Ormrod, 2001:91). The researcher used an empirical design for this research because of limited literature available on the topic. For this reason the researcher produced new knowledge through fieldwork and focused on the experience of the participants in the study (Mouton, 2001:149).

Data was collected through a literature review, which entailed reviewing key concepts in the research, and through interviews based on an interview schedule. The researcher used primary data collected through direct contact between the researcher and the participants during the interviews. The data was used to answer the research questions. The disadvantage of using this data-collection method is that the views of the participants cannot be generalised because they constitute the views of individuals.

As explained by Miles and Huberman (1994:10), the importance of well-collected qualitative data is that the focus is on naturally occurring, ordinary events in natural settings, so that the researcher has a strong handle on what 'real life' is like. A qualitative research approach was selected for this study because it contains features which enabled the researcher to obtain broad descriptions and detailed information and answers to the problem. Another reason for the researcher choosing a qualitative research approach was that it is exploratory, and the researcher aimed to listen to the participants in order to build up a picture, based on their ideas and personal experiences (Creswell, 1994:21; Taylor, 1994:208).

1.8 Target population and sampling

A target population or study population, according to Maxfield and Babbie (1995:186), consists of all the elements from which the sample is actually selected. A sample, according to De Vos, Strydom, Fouche and Delport (2005:194), comprises elements of the population considered for actual inclusion in the study. Samples are drawn because researchers want to understand the population from which they are drawn and to explain

facets of the population. A combination of probability and non-probability sampling processes was employed in the study in the form of purposive and random sampling techniques. The researcher intended to have each segment of the population represented in the sample and therefore chose to use probability sampling in addition to non-probability sampling (Leedy & Ormrod, 2005:199).

The size of the population usually makes it impractical and uneconomical to involve all the members of the population in a research project (Welman & Kruger, 2002:46). The ideal population in this research should have been all 52 investigators in the Department of Home Affairs that deal with electronic evidence. This, however, was practically impossible because they are based in different offices throughout South Africa. The researcher decided to select a sample of 25 investigators that is, Sample A who answered interview schedule A, from a team (population) of 36 special investigators situated at the Head Office in Pretoria because it was cost effective for the researcher who is also based at the Head Office. The investigators' years of experience ranged from eight to 22 years, as general investigators in the public sector. The investigators had qualifications in the legal field and in policing and some had matric as their highest level of qualification. The majority had never received formal training in computer crime investigations. The ages of the investigators ranged between 26 and 49.

The simple random sampling method as described by Leedy and Ormrod (2005:201) was used to ensure that each element had an equal chance of being selected. The sampling frame consisted of the names of 36 investigators from the Department of Home Affairs at the Head Office in Pretoria. A number was assigned to each name in the sampling frame. The researcher wrote the names of each of the investigators on separate pieces of paper, put the names in a bowl and then drew 25 names from the bowl to form a sample. This ensured that each investigator had an equal chance of being selected. The researcher regards the sample as representative of the population because she used a random sampling method.

The researcher also decided to make use of the purposive sampling method to interview experts because it gave the researcher the opportunity to make use of her own judgement and to handpick participants that were suitable for this particular research. A 'purposive sampling method' refers to a sampling method in which the researcher deliberately obtains units of analysis in such a manner that the sample obtained may be regarded as being

representative of the relevant population (De Vos *et al.*, 2005:69). The purposive sampling method was used to select five experts that is, Sample B who answered interview schedule B**,** comprising of one specialist from the South African Police Service (SAPS), one from Telkom , one from A2 Consulting in Pretoria, and two electronic evidence experts who are professors at the University of South Africa (UNISA) and the University of Cape Town (UCT) respectively.

The five experts' years of experience ranged from eight to 17 as experts in computer crime investigations in the private and public sectors. Some of the expert participants worked as specialists and others as professors specialising in the field of computer forensics. Their qualifications ranged from legal to policing and some held doctoral degrees whilst others had internationally recognised specialist qualifications in computer forensics. The ages of the expert participants ranged between 38 and 56 years old. The experts had published articles in the field of electronic forensic evidence and they also testified as electronic fraud experts in courts. The researcher is of the opinion that these were suitable candidates for responding to the aspects of the problem being researched objectively.

1.9 Data collection

The manner in which data is collected depends on the type of research and the purpose of the research. Since this is a qualitative research study, the researcher decided to use interviews and literature review as data collection techniques (McMillan & Schumacher, 2001:42). Mouton (2001:98-105) indicates that frequently used data-collection methods in qualitative research include observation, interviewing and documentary sources.

Data was collected through a literature review, which entailed reviewing the key concepts identified in the current research, and also through interviews held with the participants and based on a structured interview schedule (Flick, 2002:10; Mouton 2001:57). The researcher compiled two interview schedules whereby Sample A (25 investigators) answered the interview schedule as per annexure A and Sample B (5 experts) answered the interview schedule as per annexure B.

1.9.1 Literature search

According to Johnson (1981:18), the literature is searched for content pertaining to the subject of the research. A careful search was conducted of national and international

literature such as books, journal articles, course material, theses and dissertations, government publications, laws/statutes, encyclopaedias and literature found on the internet. The aims and research questions served as guidelines in obtaining relevant literature for the research.

The topic was divided into various concepts in an attempt to find a greater number of sources. Literature was searched for information on the concepts below and information relevant to the topic gathered:

- Forensic investigation;
- Investigation;
- Evidence;
- Document and
- Admissibility.

There was little amount of formal literature that existed in South Africa specific to the research questions or which carried the same topic. In contrast there was reasonable number of international sources that were relevant to this research. Local authors have shared a variety of information on either forensic investigation, management of physical evidence or the admissibility of evidence at trial. On the other hand, international authors have done a progressive accumulation of electronic evidence collection techniques and information on handling of electronic evidence.

1.9.2 Interviews

The researcher conducted a total of 30 face-to-face individual interviews which consisted of the 25 participants and the five expert participants, using a semi-structured interview schedule (Welman & Kruger, 2001:161). The interviews were divided into two and comprised of Sample A (25 investigators) who answered schedule as per annexure A and Sample B (5 experts) who answered schedule as per annexure B. With the semi-structured interview schedule for both Sample A and Sample B participants, the researcher made use of standard questions based on the study aims and research questions and this type of schedule also allowed the researcher to ask one or more questions to clarify the participants' thinking and also to probe the participants reasoning (Leedy & Ormrod, 2005:184). The questions under investigation guided the researcher during the selection of

questions. The researcher made use of open-ended questions, since it gave the participants the opportunity to answer comprehensively.

The researcher followed the guidelines provided by Leedy and Ormrod (2005:147-149) for conducting a productive interview:

- Make sure your interviews are representative of the group: the researcher interviewed investigators who had general knowledge of computer crime investigations and experts who had extensive experience in the collection, preservation, analysis and presentation of electronic evidence in a court of law.
- Find a suitable location: Interviews were conducted in the participants' offices, in order to make them feel comfortable by being in their own environment.
- Take a few minutes to establish a rapport: the researcher began each interview by courteously telling the participants about herself (e.g. who she is, field of work, leisure interests) to make them feel comfortable.
- Get written permission: Permission to conduct the research was obtained from the Chief Director at the Department of Home Affairs. Permission was also granted by each participant and all indicated that they would like to have their details kept confidential.
- Don't put words in people's mouths: the researcher only asked questions related to the research and noted the exact answers to the questions as provided by the participants rather than trying to change or interpret what the participants said.
- Record responses verbatim: the participants' responses were written down on the interview schedules.
- Confidentiality: for purposes of confidentiality, the researcher only refers to the participants as 'participants' in this report because they indicated that they would like to have their identity kept confidential.

1.10 Data analysis

The researcher analysed the data collected to obtain an overview of all the data. Sarantakos (1998:313) explains that the purpose of data analysis is to identify and clarify information gathered through the previous stages of the research.

The data analysis spiral from Leedy and Ormrod (2005:151) was adopted to guarantee that all data was captured accurately and common trends and patterns were identified. The approach used was as follows:

- The researcher started by analysing raw data collected through the selected data-collecting methods (interviews and literature). The data was organised and then categorised according to the key theoretical concepts 'forensic investigation', 'investigation', 'evidence', 'document' and 'admissibility', using a filing system by opening a file for each key theoretical concept, and information under each category was then filed chronologically.
- Common themes were identified in order to establish a direct and systematic approach when analysing the data (Welman & Kruger, 1999:202).
- Information was compared within categories in order to identify variations and similar meanings. Data collected was screened daily and similar data as well as variations were categorised together and where there was a need for information it was easily identified, obtained and then categorised.
- A table was used to categorise the themes: collection, preservation, analysis and presentation of electronic evidence at trial with the opinion of each investigating officer as to whether they believed the manner in which electronic evidence is collected, preserved and analysed has an effect on its admissibility at trial.

1.11 Methods to ensure validity

Validity concerns the accuracy of the questions asked, the data collected and the explanation offered. Generally it relates to the data and the analysis used in the research (Denscombe, 2002:100). The researcher ensured that the data collected was valid by consulting books, journals, periodicals, and information from the internet relevant to the aims and research questions of the research. The interviews were considered valid because the researcher interviewed experts and investigators with general knowledge about electronic evidence, with an interview schedule based on the research aims and questions. All of these factors ensured that the instrument measured what it was supposed to measure. The data was properly analysed with the use of the spiral data analysis method to ensure validity, as explained by Leedy and Ormrod (2005:151). The triangulation approach, where data is gathered from different perspectives as discussed by Leedy and Ormrod (2005:99), further strengthened the trustworthiness of the data obtained.

1.12 Methods to ensure reliability

According to Neuman (1997:138) and Sarantakos (1998:83), reliability tells us about an indicator's dependability and consistency throughout the research process, i.e. the degree to which it can be repeated. To ensure reliability, a researcher should make certain that if the same methods are used by different researchers and/or at different times, they should still produce similar results. The researcher used a semi-structured interview schedule to ensure consistency throughout the interviews. The interview schedule assisted the researcher to provide accurate results that do not vary from interview to interview; in other words, the same criteria for questions were used for all the participants, as explained by Denscombe (2002:100).

The interviewer did not lead the participants to answer in a specific manner, thus not leading them in a specific direction. This ensured that when different researchers conduct the same research by means of the same interview schedule as measurement tool they are likely to obtain similar results. The degree of consistency with which participants answered the questions played a role in ensuring reliability. Data relevant to the aims and research questions was collected during the literature search to ensure consistency in the data-collection process.

1.13 Ethical considerations

Ethical guidelines serve as standards and the basis upon which each researcher ought to evaluate his/her own conduct (De Vos, 1998:24). The process of ensuring that the research conformed to the necessary ethical requirements was guided by the guidelines provided by Leedy and Ormrod (2005:101) and the researcher carried out the following:

- Participants were protected from harm and not exposed to unnecessary stress, embarrassment or loss of self-esteem. The participants were asked to stop the interview at any stage if they felt uncomfortable.
- The researcher sought consent from and ensured that the participants were given sufficient information about the research, which allowed them to make an informed decision, and participation was voluntarily.

- The right to privacy was respected and the researcher allocated a code number to each of the participants to honour their privacy. In the research report, the responses by the participants are not disclosed in a manner that exposes a specific participant.
- The researcher remained honest throughout the study and did not fabricate data to support a specific finding. Proper referencing was carried out, sources of information acknowledged and the researcher observed the rules of the Reference Method for UNISA (2004:1) and did not plagiarise information (Mouton, 2001:240).

1.14 Research structure

The report discusses the research concepts and answers the research questions as divided into the following chapters:

- **Chapter 1 – General Orientation**

  The first chapter looks at the research problem and discusses the principal aim of the research followed by the purpose of the research. The chapter also explores the research questions to be answered and defines concepts used in the research in order to prevent any misunderstanding. The chapter then discusses the value of the research. This is followed by a detailed discussion of the research design and approach to provide the overall structure for the procedures that the researcher followed. This in turn leads to a discussion on target population and sampling to provide information about the elements of the population considered for actual inclusion in the study. This chapter also reflects on the manner in which data was collected and analysed to identify and clarify information gathered through the stages of the research. The last part of the chapter focuses on the methods used to ensure validity and reliability. The chapter concludes by presenting that the research conformed to the necessary ethical requirements.

- **Chapter 2 – Forensic Investigation**

  This chapter explores the concept ‘forensic investigation’ and provides information for a better understanding of the role of an investigator and the mandate to investigate. The researcher briefly discusses the responsibilities and qualities of a good investigator. The difference between forensic investigations and criminal investigations is also discussed in this chapter. The chapter concludes by presenting the objectives of investigations.

- **Chapter 3 – Electronic Evidence**

  This chapter defines the concept ‘electronic evidence’. The researcher discusses types of evidence and the classification of electronic evidence under these types. The last part of the chapter focuses on the difference between paper and electronic evidence.

- **Chapter 4 – Collection of Electronic Evidence**

  This chapter explores how electronic evidence can be collected without compromising its integrity or credibility at trial. This chapter therefore begins with a discussion on the investigation and collection of electronic evidence. This in turn leads to a discussion on the importance of maintaining a chain of custody. The researcher also discusses the importance of obtaining a search warrant for the purposes of collecting evidence and the procedure for obtaining such a warrant. This is then followed by a discussion on how experts can assist in the collection, preservation, analysis and presentation of electronic evidence.

- **Chapter 5 – Legal Requirements for Admissibility of Electronic Evidence**

  The legal requirements for admissibility of electronic evidence at a trial are discussed in this chapter. The chapter begins with a discussion of the South African legal framework on electronic evidence. This is followed by a detailed discussion of the requirements for admissibility of electronic evidence. This leads to a brief discussion on hearsay evidence. The chapter ends with an explanation of the role of an investigator in presenting electronic evidence in court and the challenges brought about by electronic evidence in court.

- **Chapter 6 –Findings and Recommendations**

  This chapter reflects the findings of the research project and the recommendations for implementation of the findings as well as suggestions for further research.

CHAPTER 2
FORENSIC INVESTIGATION

2.1 Introduction

According to Zysman (2006:4), "forensic investigation involves the utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law". Shah (2002:10) explains that forensic investigation requires specific skills, the use of human instinct and intellectual analytical capability, which accordingly makes it a unique profession. As observed by Kennedy (2004:1), forensic investigation can therefore be considered a specialised field.

Van Rooyen (2004:16) states that in the course of an investigation, investigators must always execute their mandate within the ambit of the law and its limitations. Swanson, Chamelin and Territo (2003:28) point out that in conducting an investigation, the investigators should strive to search for the truth. Joubert (2001:268) maintains that evidence must be collected in accordance with the Constitution and relevant laws. In light of the above, and as indicated by Shah (2002:39), the investigator should always recognise the law and human rights guaranteed to the accused persons.

This chapter discusses and analyses the meaning of the concept 'forensic investigation'. This in turn leads to a discussion on what a forensic investigator is. The researcher further explains who has the mandate to conduct investigations. This is followed by a discussion of the qualities and the responsibilities of an investigator. For the purpose of this study the term investigator will also include and refer to a crime investigator, forensic investigator and a corporate investigator. The researcher also tries to determine whether there is a difference between the two concepts of forensic investigation and criminal investigation. The chapter concludes with a discussion on the objectives of forensic investigation.

2.2 Forensic investigation

McKenzie (1996:5) explains that the word 'forensic' is derived from the Latin word *forensic*, meaning 'giving the opportunity to debate'. As pointed out by Karagiozis and Sgaglio (2005:3), the Romans debated their legal cases and had the verdicts announced in public. According to the authors, these debates are what the term 'forensic' refers to. The

researcher, however, is of the opinion that the explanation offered by Van Rooyen (2004:7) is more complete. Van Rooyen (2004:7) explains that, although dictionaries differ slightly in their definition of the word 'forensic', the true meaning is twofold: on the one hand it refers to "courts of law, juristic or court directed and relating to the application of science to decide questions arising from crime or litigation". On the other hand, it incorporates the task of examination or analysis. Thornhill (1995:5) further explains that the word 'forensic' by itself is defined in part as pertaining to, connected with, or used in courts of law or public discussion or debate.

It is the researcher's experience that since the enormous growth of investigation in the private and corporate sectors the term 'forensic investigation' has become very popular and that private sectors will often refer to an investigation department/unit as a 'forensic investigation department'. Before this growth of investigation in the private sectors, the term 'forensic' was more often associated with the South African Police Service Forensic Science Laboratory (SAPSFSL). The term 'forensic investigation' will include criminal investigation and the general term 'investigation' for the purpose of this research.

The above definitions of forensic investigation were also emphasised by the majority of 25 participants in this study who were all involved in investigation. When asked the question "What is forensic investigation?", Nine participants said that it is a field in which an investigator legally collects evidence and facts about a particular case under investigation. These participants further mentioned that the evidence is collected with the purpose that it is to be presented in a court of law. Four participants concurred with this view and said that forensic investigation is the use of specialist skills to obtain evidence about a crime that has been committed and the successful use of such evidence for the prosecution of offenders. This confirms the views of Lambrechts (2001:93) and Gardner (2005:1), who state that forensic investigation is aimed at constituting criminal proceedings.

Three participants defined a forensic investigation as an investigation of any serious and complex crime and also mentioned that this field requires specialist skills and techniques. This supports Fisher (2004:73) and Lambrechts' (2001:93) view that a proper investigation that can lead to presentation of evidence in a court of law can only be ensured through a combination of scientific and investigative methods and techniques.

Seven participants said that the concept refers to many other forms of investigation, and according to the participants this includes the investigation of “computer crimes” whilst the others said it includes investigating “financial crimes” and “uncovering scientific or biological evidence”. Only two participants diverged: one of these participants said that forensic investigation is “the scientific or biological investigation of human bodies” and the other said that forensic investigation is about determining any biological evidence like hair or blood samples left at a crime scene. These definitions are understandable considering the former use of the concept ‘forensic’ as explained above. It is evident from the definitions provided by the participants that they are familiar with the definition of the concept ‘forensic investigation’.

The researcher makes a conclusion that forensic investigation is a process that outlines the extensive intellectual capacity in tackling and proving incidence of criminal activities. It consist of a combination of scientific and investigative methods and techniques to confirm a crime that has been committed and the successful use of collected evidence for the prosecution of offenders.

2.3 Investigator/detective

Holmes (2006:2) explores the history of detectives, explaining that the first police detectives were established in England during the seventeenth century and that this was followed by France in the eighteenth century. Palmiotto (1998:4), in tracing how detectives were established in France, suggests that the detectives were founded by a former convict who believed that it takes one criminal to catch another.

The evolution of detectives as observed by the researcher can be attributed to the growth in criminal activities that extended beyond country borders, which as a result necessitated cooperation by states to address international criminal activity. This situation, as shown by studies like O’Hara (1962:22), led to the establishment of the International Criminal Police Commission in the nineteenth century, today known as ‘INTERPOL’. The concept of specialised criminal investigation, as indicated by Ward (1975:12), started developing during this period. According to Karagiozis and Sgaglio (2005:4), forensic investigation has even earlier roots, starting in ancient Greece when the king suspected the royal jeweler of defrauding him in the making of his crown.

Furthermore, a forensic investigator often referred to as a 'detective' is defined by Van Rooyen (2004:6) as a law enforcement officer who investigates crime. Callanan (1992:1) explains that the word 'detective' is derived from the Greek word *detergere*, which can be interpreted as "expose" or "uncover". The American Heritage Dictionary of the English Language (2003:324) defines an investigator as either a police officer or anyone else who conducts an investigation.

As observed by the researcher, forensic investigators operate within the confines of the law in carrying out their mandate. It is therefore important to explore the mandate of investigators to investigate crimes.

2.3.1 The mandate to investigate

It is stated in the South African Police Service Act 68 of 1988(b) that the investigation of all committed crimes lies with the police. In *S v Botha and Others* (1) 1995 (2) SARC 598 (w) the defence attorney also referred to section 215(b) of the South African Interim Constitution Act 200 of 1993 and argued that according to the section only police officials could investigate crime and that no other body possessed this authority. Serious criticism can be raised against both the South African Police Service Act 68 of 1988(b) and section 215(b) of the South African Interim Constitution Act 200 of 1993, in view of the fact that, as a study conducted by Shah (2002:39) has shown, there are many other role players in the fight against crime. Nevertheless such criticism will not be dealt with in this research.

Through experience in investigations the researcher is familiar with the fact that the corporate, private security and public sectors also have a legal responsibility to conduct criminal investigations. This supports the view of Van Rooyen (2004:1) when mentioning that corporate bodies, government departments and the private investigation industry have created their own internal investigation structures. An explanation of this is that various statutes also confer a certain degree of investigative powers on corporate bodies and government departments, as noted by Swanepoel (2001:3-7).

With regard to the mandate to investigate, in *S v Botha and Others* (1) 1995 (2) SARC 598 (w) the judge conversely ruled that it is not the purpose of section 215(b) to prevent someone who is not a member of South African Police Service (SAPS) from conducting an investigation. The judge said that various institutions conduct their own investigations and

then hand the evidence over to the police. In addition, as realized by the researcher, those institutions can only use the evidence for internal disciplinary actions and have to rely on the police if they wish to press criminal charges against an accused.

The 25 participants were asked the question "Who has the mandate to conduct investigations?" 19 mentioned the "South African Police Service (SAPS)", "Directorate of Special Operations", "South African Secret Service (SASS)", "National Intelligence Agency (NIA)", "South African National Defence Force (SANDF)" and "South African Revenue Service (SARS)". Five participants also indicated that the corporate sector and certain government departments can conduct investigations. One participant said "the mandate to conduct investigation is vested to law enforcement and other organizations mandated by legislation to conduct investigations".

In addition the majority of the participants emphasised that the corporate sector and certain government departments even if mandated by legislation to conduct investigations, have limited powers to investigate. It is critical to note that even though these institutions conduct their own investigations, their findings are still delivered to the SAPS for the institution of prosecution, as pointed out by Van Rooyen (2004:3).

It is therefore evident that the police service is not the only body mandated to conduct investigations. Some of the institutions that have a mandate to investigate are briefly discussed below.

2.3.1.1 The South African Police Service

According to Shah (2002:1), the police have been given certain legal powers to enable them to perform their task of finding out clues to offences and working out these clues to fix the problem. Section 205 (3) of the Constitution of the Republic of South Africa 108 of 1996(a) recognises the South African Police Service as the primary law enforcement agency with the power to investigate crime and to uphold and enforce the law, amongst other powers invested in them (South Africa, 1996:sec.205(3)). The Criminal Procedure Act 51 of 1977 also confers extensive investigative powers on the South African Police Service. This, however, does not imply that only the police have exclusive rights to investigate, as noted by Swanepoel (2001:3).

2.3.1.2 Special Investigating Unit

The Special Investigating Unit and Special Tribunal Act 74 of 1996 (b) confer powers on the Special Investigating Unit to investigate conduct of serious malpractices or maladministration against the state which may harm the interest of the public. The collected evidence is then referred to the prosecuting authority as it is believed by Marud (2004:28) that all role players should share information in their efforts to combat crime.

2.3.1.3 Corporate investigators

The Private Security Industry Regulation Act 56 of 2001 confers powers on corporate investigators. The investigators can conduct investigations relating to wrongdoing by officials. Corporate investigators have the power to obtain statements and documentary evidence and to serve as witnesses. As experienced by the researcher in practice, the investigators prepare preliminary investigations and forward their findings to the police for finalisation and presentation in court, the reason being that the Criminal Procedure Act 51 of 1977 stipulates that only the police can bring a case before a criminal court**.**

2.3.1.4 Department of Home Affairs

The Department of Home Affairs is an example of a government department that has an internal investigation unit. The internal unit of the Department of Home Affairs is responsible for the investigation of the theft or unauthorised production of face value documents and immigration-related offences under the Immigration Act 13 of 2002(b) as well as corruption under the Prevention and Combating of Corrupt Activities Act 12 of 2004 Although the investigators have powers to effect arrests, collect evidence from open sources of information, and conduct searches and seizures, their powers are still limited. The investigators therefore work in collaboration with the South African Police Service to have the perpetrator(s) prosecuted.

2.3.1.5 External auditors

The Auditing Profession Act 126 of 2005 provides for the investigations of unlawful acts or omissions by management responsible for an entity. Auditors investigate fraudulent activities, corruption and maladministration in connection with the finances of an entity. The evidence collected is handed over to the police and the auditors are used to provide expert evidence in court.

The above discussion leads to the conclusion that, although the abovementioned organisations are capable of conducting their own investigation, they still need to rely on the police to assist should they decide to charge the offenders criminally.

As much as investigators from organisations outside the South African Police Service can conduct investigations, it is expected of them to have certain qualities in order to carry out their mandate effectively. The qualities of an investigator are therefore the next point of discussion.

2.3.2 Qualities of an investigator

According to Lee, Palmbach and Miller (2003:1) the basis of investigations is based on the ability of the crime scene investigator to recognise the potential and importance of physical evidence at the crime scene. This is an indication that intuition and an eye for what needs to be done as also suggested by Fisher and Fisher (2003:50) are some of the qualities required from an investigator. Some of the qualities of an investigator are brought to light in the study by Swanson *et al.* (2003:29), as follows:

- "Being able to not act out of malice or bias;
- Discipline;
- Use of own initiative and resourcefulness;
- Being ethical and always using legally approved methods and
- Ability to influence and win the confidence of the people they interact with."

The 25 participants also provided diverse responses to the question: "What qualities should an investigator have?" 17 participants indicated that an investigator must be objective and independent in thinking and should remain unbiased. This supports the view of Vadackumchery (2003:46) that sincerity, honesty and integrity are vital qualities of an investigator.

Six participants believed that investigators should have good organisational skills and others emphasised that the investigator should have good oral and written communication. One participant said an investigator must pay attention to detail. This participant explained that the investigator must have a checklist covering all the details about the investigation that might be overlooked and should also follow procedures accurately to make sure the

investigation is conducted properly. Another participant confirmed this view and said that the ability to be thorough in conducting an investigation is one of the qualities of a good investigator.

It can be deduced from the interviews that an investigator should be endowed with each of the qualities mentioned by the participants in varying degrees, as also mentioned by Sennewald and Tsukayama (2006:18) that "invariably a successful investigator will posses in varying degrees each of this traits, either as innate or learned qualities". It can, however, be argued that some qualities are more essential to an investigator than others.

It is worth noting as perceived by the researcher that, although investigators can possess the essential skills that empower them to conduct investigations effectively, they are also entrusted with certain responsibilities in their field as investigators. The responsibilities of an investigator are discussed below.

2.3.3 Responsibilities of an investigator

According to Simms and Petersen (1991:216), an investigator is responsible for the following:

- "Identifying the occurrence of offenses;
- Compiling reports on the circumstances surrounding the occurrence;
- Interviewing victims, witnesses and suspects with the objective of identifying the offender and
- Gathering sufficient evidence to allow prosecution to proceed."

The main responsibilities of an investigator are summarised by Horswell (2004:69) as follows:

- "Assessment of the crime scene;
- Control of the crime scene;
- Examination of the crime scene;
- Interpretation of the evidence;
- Recording of the crime scene;
- Evidence collection and
- Case management."

Generally there are a number of fundamental responsibilities as mentioned by Simms and Petersen (1991:216) as well as Horswell (2004:69) that virtually all investigators have in common. This is an indication that it is important to understand what investigators do since they are important role players in investigations. In the study conducted by Kipper (2007:55) with regard to computer crimes, it was found that an investigator is responsible for managing the preservation, collection, examination, analysis and reporting of computer evidence. These responsibilities as mentioned by Swanson *et al.* (2003:28), can be accomplished through the criminal investigation process which according to (Osterburg & Ward 2000) involves outlining the responsibilities of an investigator in conducting investigations.

In order to determine the responsibilities of an investigator as seen by the sample of the study, the 25 participants were asked the question: "What are the responsibilities of an investigator?" 19 participants said investigators are responsible for "collecting evidence", "securing evidence", "documenting evidence", "presenting evidence in court" and "ensuring that all witnesses appear at the trial". Three participants explained that investigators search for the truth, compile dockets for court, assist the prosecution to formulate charges and ensure that the perpetrators face prosecution. One participant viewed the investigator as a person responsible for offering protection and said that an investigator has to protect the community from harm. According to this participant, "the investigator will have to find information about crime to be committed and ensure that the perpetrators are arrested before the victims are harmed". Two participants were too general in their responses to provide a reasonable description of an investigator's responsibilities, stating "that the investigator provides support to other law enforcement agencies" and that "they enforce the law".

It is apparent from the information obtained during the interviews that the responsibilities of an investigator are extensive. This confirms the view of Horswell (2004:57) who states that the field of investigation places exceptionally high demands on investigators. The responsibilities as analysed by Van Rooyen (2004:19) entail answering the questions: 'Who?' 'What?' 'Where?' 'When?' 'Why?' and 'How?' in relation to conducting a proper investigation. The study reported on in Bailey (1995:160) also point out that the biggest

responsibility in answering the questions mentioned by Van Rooyen (2004:19) above about an investigation lies with the investigator.

The responsibilities of an investigator as discussed above provide an overview of what is expected from an investigator when conducting an investigation. The next topic will focus on the difference between forensic investigation and criminal investigation.

2.4 The difference between forensic investigation and criminal investigation

Van Rooyen (2004:25) describes the investigation of a crime as "a systematic, organized search for the truth". It can also be argued that the end result of a criminal investigation (as detected by the researcher) is to initiate criminal proceedings. This view is expressed by authors such as Lambrechts (2001:93), who explains that forensic investigation is an investigation aimed at instituting court proceedings whether criminal or civil, and Gardner (2005:1), who states that the aim of forensic investigation is to initiate a litigation process. The problem with Van Rooyen's (2004:25) definition of criminal investigation is that it falls short of the aim of directing the investigation towards prosecution. This contradicts the studies undertaken by Lambrechts (2001:93) and Gardner (2005:1) and also Joubert (2001:223), who in addition mentions that crime investigation begins when a crime is committed and continues until the start of a trial.

The researcher therefore concludes, based on her own experience and information from reviewed studies, that there is no clear and outstanding distinction between the two concepts 'criminal investigation' and 'forensic investigation'. The concept 'criminal investigation', however, only covers investigations of a criminal nature, while forensic investigations can also include civil investigations, as pointed out by Lambrechts (2001:93).

For the purpose of this study the term investigator will also include and refer to a crime investigator, forensic investigator and a corporate investigator.

2.5 Objectives of investigation

According to Bennett and Hess (2004:05), the objective of investigation is to determine if indeed an offence been committed then identify and apprehend the suspect, recover the stolen property and assist in the prosecution of the person charged with the crime. Fisher

(2004:48) and Golden, Skalak and Clayton (2006:111) concur with this view and add that the objective of investigation is to prove an unlawful action. According to Marais and Van Rooyen (1994:19) the objectives of an investigation is situation identification which involves making an observation at a crime scene to identify the crime committed, which is followed by gathering evidence. Consequently, the objective of crime investigation as mentioned by Weston, Lushbaugh and Wells (2000:2) is to determine the truth, as far as it can be discovered in any inquiry.

The objectives of investigation namely; identification of crime, collection of evidence, identification of the suspect, securing the attendance of the accused in court, recovery of stolen property and prosecution are herewith briefly discussed.

2.5.1 Identification of crime

According to Horswell (2004:9), the investigator has first to establish whether an offence has in fact been committed and, if so, then to determine the nature of the offence. Byrd (2004:1) explains that before investigators gather information, they should start by identifying all relevant information that can give an indication of the crime committed. The author further explains that investigators should be able to recognise and identify all relevant information that can shed light on the crime committed before such information can be collected. The evidence will then be considered to determine the unlawful nature of the event, as noted by Horswell (2004:7).

2.5.2 Collection of evidence

The next objective of investigation is to collect evidence. Ogle (2004:20) and Fisher (2004:55) mention that the investigator should always exercise reasonable care when gathering evidence. Fisher (2004:53) explains that each piece of evidence should be identified, collected and preserved as a separate entity. Genge (2002:8) and Fisher (2004:53) caution that the physical evidence must be collected with care to protect its identity and integrity.

Byrd (2004:1) provides the following as reasons for gathering evidence:

- "To prove that a crime has been committed;
- To establish any key elements of a crime;

- To link a suspect to a crime scene;
- To establish the identity of a victim or suspect;
- To corroborate verbal witness testimony and
- To acquit the innocent."

2.5.3 Identification of the suspect

The other objective of investigation is the identification of a suspect. Dowling (1997:2) explains that it is the primary task of the investigator to identify who committed the crime. Van der Westhuizen (1996:6) provides another important aspect, which is that the investigator should link the suspect to the information and facts collected during the investigation. Once the suspect is identified, an arrest can then be made.

2.5.4 Securing the attendance of the accused in court

Van der Westhuizen (1996:7) points out that the purpose of the arrest is to ensure the presence of the accused at the trial. This, however, starts with the investigator identifying the person who has committed the crime, as noted by Lee and Harris (2000:14). The researcher's experience suggests that an arrest can only be effected once all the relevant information has been collected, the crime identified and the suspect linked to the crime. Alternatively, the presence of the accused at the trial can also be ensured by issuing a summons, a written notification and a deed of accusation in accordance with section 38 of the Criminal Procedure Act 51 of 1977.

2.5.5 Recovery of stolen property

Another objective of investigation is to recover stolen property. According to Van der Westhuizen (1996:7), the purpose of recovering the stolen property is to minimise the loss suffered by the victim and, most importantly, to present the recovered property as evidence at the trial.

2.5.6 Prosecution

The last objective of investigation is prosecution. As advised by Bester (2002:29), the investigator should collect and document enough evidence that links the accused to the crime as this will help ensure successful prosecution and conviction. Van der Westhuizen (1996:7) explains that successful prosecution is dependent on the expertise and competency

of the investigator who has conducted the investigation. This is because the investigator is the one who can assist the prosecutor to present evidence and to reconstruct the crime in court, as indicated by Palm (2000:35).

To determine the objectives of investigation from the point of view of the sample of investigators, the 25 participants were asked the question: “What are the objectives of a investigation?” 22 participants said “investigate offences”, “collect evidence”, “apprehend criminals”, and “initiate prosecution” and “ensure prosecution of the offenders”. Two participants pointed out that the objective of investigation is to collect evidence by conducting interviews with suspects, witnesses and victims. These participants explained that this can also involve the issuing of a summons to compel service providers or those in possession of information that can assist in the investigation to provide such information. One participant said investigation serves as deterrence for people who intend to commit crime.

The participants did not mention anything about recovering stolen property. An explanation of this could be that they rely mostly on the South African Police Service to institute criminal proceedings and as a result assume that the police will initiate the process of tracing hidden assets and recovering stolen goods. Dowling (1997:4) urges the investigator always to make an effort to recover stolen property. Investigators also have the option of engaging a prosecutor to utilise section 300 of the Criminal Procedure Act 51 of 1977 to request the court to recover losses.

2.6 Summary

This chapter has revealed that investigation is a highly specialised field. In the field of investigation, the investigator uses his special skills to obtain factual information about an allegation and to collect information and evidence for court purposes. It is therefore important for an investigator to understand what investigation entails and to have a clear understanding of the objectives of investigation.

In the next chapter the researcher discusses electronic evidence and its purpose in investigation.

CHAPTER 3
ELECTRONIC EVIDENCE

3.1 Introduction

Keane (2000:1) indicates that evidence is information which tends to prove facts in a court of law. Van Rooyen (2004:9) further explains that evidence may be presented either orally or physically by means of documents that are admissible to assist the court to reach a conclusion. Accordingly, the concept 'electronic evidence' in the context of the above-mentioned definition of evidence is described by Volonino (2003:7) as referring to information that is stored electronically on a computer and that can be used as evidence at trial.

This chapter begins with a discussion of the concept 'electronic evidence'. This is followed by a brief discussion of the types of evidence available and the researcher then looks at where electronic evidence resorts under these types of evidence. The chapter concludes with a comparison between electronic evidence and paper evidence.

3.2 Electronic evidence

Kovacich and Boni (2000:5) point out that nowadays people are increasingly computer literate and use computers in every aspect of their lives. According to Lange and Nimsger (2004:1-4), the advancement of computers has therefore created an entirely new source of evidence in investigations referred to as 'electronic evidence'.

Electronic evidence is defined by Casey (2000:1) as any electronic information created on a computer that can link a crime and a suspect. It should however be noted that other possible locations where electronic evidence can reside in the graphic provided by Lange and Nimsger (2009:72) also includes but not limited to; optical disks, floppy disks, remote internet storage, handheld devices, memory cards, network servers and emails. This kind of evidence as indicated by Silvernail (1997:176-177) may be created at any stage once a person starts to use and enter information into a computer. As pointed out by Chisum and Turvey (2000:11), this is confirmed by the Locard principle in the field of investigation, which explains that when two objects touch each other a transfer of trails occurs. This

emphasises the fact that electronic evidence can provide a critical link between the perpetrator and the victim, as noted by Wang (2007:8).

To determine the knowledge of the 25 participants on electronic evidence, the researcher asked the question "What is electronic evidence?" In answer, 16 of the participants said electronic evidence is any information stored or transmitted in an electronic form and retrieved later to be used at trial. Four participants viewed electronic evidence as evidence that is stored in a computer and that can be used to determine the truth of an allegation in a court of law. This view confirms the definition of electronic evidence by Overly (1999:1), who states that electronic evidence is "information stored in electronic form that is relevant to the issues in a particular litigation". Velasco (2007:6) explains that the relevant electronic evidence must be gathered in a method that will be both admissible and justifiable in court. Two participants said that electronic evidence is evidence introduced in a trial from a computer system and intended to prove a fact in issue. Three said it is evidence retrieved from a computer system.

The majority of the 25 participants demonstrated a good understanding of the concept 'electronic evidence'. Although they provided different meanings based on their understanding of the concept, they all made reference to information stored in a computer system and used as evidence in court.

For a better understanding of the classification of electronic evidence, it is critical to discuss other types of evidence.

3.3 Types of evidence

The various types of evidence that an investigator has to deal with in criminal investigation can be broadly divided into the following categories:

- Oral evidence: this is evidence that originates from interviews or statements or that is given verbally (Van Rooyen, 2004:9).
- Physical evidence: this evidence originates from a large variety of physical objects such as computers, fingerprints, handwriting, photographs and anything that could indicate that a crime has been committed (Van Rooyen, 2004:8).

- Expert evidence: this is evidence presented by experts and usually contains their opinions and conclusions drawn from their field of expertise (Shah, 2002:6-7). It remains the prerogative of the courts whether to accept or not accept the opinion of an expert, as noted by McGregor and Hobbs (1998:8).

The 25 participants did not group the types of evidence into the broad categories mentioned above, but when asked the question "What are the types of evidence?" 23 participants listed "photographs", "documents", "written statements", "business records like bank statements", "material objects such as a computer and hard drives", and two mentioned "sound and video recordings".

It is evident that the 25 participants mentioned evidence from their own practical experience, as they did not refer to the specific categories of evidence which include oral, physical and expert evidence. Some of the participants also pointed out that it is important for the evidence to have a direct bearing on the crime committed. Another point of great importance, as mentioned by Van Rooyen (2004:94), is that all evidence recovered at a crime scene provides the investigators with leads to follow in the course of their investigation. Horswell (2004:7) supports this view and mentions that evidence can be used to:

- "Prove that a crime has been committed;
- Establish key elements of a crime;
- Be the decisive element in determining guilt or innocence;
- Provide the lead to the perpetrator of a crime;
- Provide a link in a chain of circumstantial evidence;
- Corroborate other evidence and
- Test the statements of complainants, witnesses or suspects."

The above is a reflection of the importance of the use of evidence in the investigation process. It is therefore also important to elaborate on the classification of electronic evidence as a useful form of evidence.

3.4 Classification of electronic evidence

Stephenson (2000:86) classifies information coming out of a computer as hearsay because it is not directly seen from the computer and the only person who has direct knowledge of it is the person who created it. The author further mentions that because this evidence is not based on personal observation of the offence, it is therefore circumstantial. Circumstantial evidence is defined by Cross (2008:626) as observation or knowledge of facts that tends to support a conclusion indirectly but does not prove it definitely and therefore is not based on personal observation of the offence.

Notwithstanding the above, Cardwell, Clinton, Cohen, Collins, Cornell, Cross, Depew, Ehuan, Gregg, Jean, O'Shea, Reis, Reyes, Schuler, Schneider, Schroader, Varsalone, Wiles and Wright (2007:269) maintain that electronic evidence resorts under physical evidence since the legal system views both computer and information generated by that computer as property.

To determine the classification of electronic evidence the 25 participants and five expert participants were asked the question "Where does electronic evidence resort under the categories or types of evidence?" The first section of reporting deals with the 25 participants and the second one deal with the five experts. From the responses provided by the 25 participants, four of the participants said that electronic evidence can be classified as circumstantial evidence. These participants elaborated that this is because it is not the originator of the evidence that provides the evidence in court but a third person; this makes it circumstantial evidence.

Seven participants said that electronic evidence is documentary evidence because it is presented in court in the form of documents. 11 participants viewed electronic evidence as physical evidence. One participant explained that this is because the computer and information retrieved out of it are all objects that can establish that a crime has been committed and can provide a link between a crime and the person who committed the crime. Two participants lacked knowledge and said they did not have an idea. The possible broad reason for the lack of knowledge on the part of the two out of the 25 participants might be linked to different interpretations of computer evidence and to inadequate training on this aspect of investigation.

As mentioned above, the responses by the 25 participants are followed by those of the expert participants. One participant reported that the courts do not know how to classify electronic evidence. This participant indicated that at times the courts classify electronic evidence as documentary evidence and, depending on how the evidence is presented in court, sometimes it is regarded as real evidence. The latter view was confirmed by three participants who said that, for instance, a computer printout may be dealt with as documentary evidence or as a photograph and may be dealt with as real evidence; it all depends on the facts of each case. The three abovementioned participants classified electronic evidence as real or documentary. Another participant said that electronic evidence is classified as real evidence.The 25 participants had different views on this important aspect of electronic evidence. However, according to some of the expert participants, the facts of each case can assist in determining the type of evidence the electronically generated information represents.

With regard to the classification of electronic evidence, in *S v Ndiki and Others* 2008 (2) SACR 252 (Ck), Justice Van Zyl dealt with electronic evidence as real evidence because the computer that generated the electronic evidence had been programmed to generate such information on its own without human interference. The same principle was also applied in *Ex Parte Rosch* 1998 1 AII SA 319 (W), where the court treated a computer printout as real evidence because it was generated automatically without any input or information from a human being. Some of the expert participants mentioned that, in instances where a computer is operated by a person to generate the evidence, such evidence will be classified as documentary evidence. As an example, in *S v De Villiers* 1993 (1) SACR 574 (Nm), the court found that information contained in a computer printout where such information had a human source is regarded as a document.

Justice Van Zyl in *S v Ndiki and Others* 2008 (2) SACR 252 (Ck) validates the views of some of the expert participants by mentioning that the evidence in issue should be closely examined to determine the kind of evidence that is being dealt with and the requirements for its admissibility. One of the expert participants then suggested that a new category of evidence needed to be created in order to accommodate electronic evidence. In view of the fact that there seems to be a confusion by the courts on whether to classify electronic evidence as real or documentary evidence, it is necessary to examine whether there is a difference between electronic evidence and paper evidence.

3.5 Electronic evidence versus paper evidence

Neumeier, Hansen and Dmitrieva (2003:2) mention that when paper is used to store incriminating information, a witness's statement about the history of a particular document is commonly relied on. However, the situation is different with information that is stored on a computer. Unlike paper evidence, most fraudulent electronic offences, as indicated by Balkin, Grimmelmmann, Katz, Kozolvski and Zarsky (2007:225), are not witnessed; this means that the underlying evidence relied on is electronic evidence.

To determine the views of the 25 participants and the five expert participants on this topic, the researcher asked the question "What is the difference between electronic evidence and paper evidence?" The first section of reporting deals with the 25 participants and the second one deal with the five experts. From the responses provided by the 25 participants, 18 participants said paper evidence is stored on documents and electronic evidence is stored on a computer. Five said case files are paper evidence but memory sticks and compact disks are electronic evidence. Two out of the 25 said they never thought that paper and electronic evidence needs to be differentiated.

In response to the same question the five expert participants provided the following responses; two expert participants pointed out that both the computer and paper are used to store information and that any information stored on a computer can be printed on paper and as a result can be treated as a document. One participant was of the same view and added that, although the information from a computer can be printed on paper and treated as a document, this does not mean that these types of evidence can be treated the same because of their physical differences.

Two expert participants reported that every piece of information captured electronically remains on a computer hard drive although it might appear deleted from the surface, whilst on the other hand a paper document can be completely destroyed, for example by shredding it. One of these above expert participants additionally pointed out that the Electronic Communications and Transactions Act 25 of 2002 is meant to address electronic evidence, which is not catered for in the existing rules of the law of evidence because these rules were designed specifically for paper documents. According to the expert participant, this is an indication that there is a distinction between electronic and paper evidence.

With regard to the difference between paper and electronic documents, the explanation provided by these expert participants on how the information remain stored in the computer system even when deleted is discussed later in this chapter, under the subheading "Deletion of electronic evidence". The distinction between electronic evidence and paper evidence is briefly discussed below.

3.5.1 Embedded information

The first distinction between paper and electronic evidence is in the history of any electronic document, which remains embedded in the computer system. "Embedded information describes how, when and by whom an electronic document was created, modified and transmitted" LexisNexis White Paper (LexisNexis, 2007:2). As a result this embedded information creates a link between the creator and the user of information, as indicated by Taylor (2003:3). Gallagher and Aro (2005:8) emphasise that the embedded codes remain stored on a computer and can track usage and transmission of information back to the originator of the electronic information. On the other hand, as mentioned by Raysman and Brown (1984:26), a printed document may not show its history, for instance: the origins, contacts or edits carried out in the document. Parlade (2004:6) explains that unlike paper documents electronic documents contain embedded data.

This embedded data contained in a document, as observed by the researcher in practice, has exposed an official who sent an anonymous offensive mail by attaching a document that was created from his computer. Upon investigation, the embedded data from the electronic document showed the particulars of the author. Raysman and Brown (1984:26) also state that one can surely get background information about the origins of electronic evidence. Shira, Scheindlin and Rabkin (2000:327-338) validate this view by mentioning that electronic information potentially contains a wealth of hidden information that simply does not exist in a paper document. For instance, in the case of the official who sent the anonymous offensive mail, if the official had printed the document and circulated it physically without being noticed, it would have been difficult to trace the author because the paper document does not show information embedded in it.

A deduction can be made from the above information that it is not easy to destroy electronic evidence, and this is of great benefit to an investigation. The next distinguishing

factor between paper and electronic evidence relating to the deletion of electronic evidence provides further clarity in this regard.

3.5.2 Deletion of electronic evidence

According to Robbins (1999:411), it is true that electronic information generally is very mutable and easily altered with a few simple keystrokes; however, it is not easy to remove or delete an electronic document totally. Lange and Nimsger (2004:6) explain that a trace of electronic evidence tends to remain on the computer's hard drive even after deletion of the information. As mentioned by Kozushko (2003:6), copies can remain in hidden places when criminals attempt to destroy electronic evidence. In contrast, Balkin *et al.* (2007:213) maintain that electronic evidence is easy to destroy and alter. This last view contradicts the views of the five expert participants, who provided detailed information on how a computer stores information. This information provided by the experts, as raised earlier on, is briefly discussed in this sub-section.

Three out of the five participants explained that a computer stores information in patterns of 0s and 1s, referred to as 'binary numbers'. One of these three participants explained that the computer hard drive has a round flat disk coated on both sides with a magnetic material, with each side capable of storing billions of data. According to the participant, once a file containing data is deleted on the computer, the system only deletes the first letter of the file name but the old data remains stored in the computer.

Two participants reported that old data can only be deleted when new information is written on top of it. The two participants further mentioned that it is unlikely that the space where old data is stored can be successfully overwritten with new data because data is randomly stored in the millions of other available spaces on the computer. This means that portions of deleted files can still be recovered long after they have been deleted from the computer. This makes computer evidence unique and valuable for investigation purposes, as in the researcher's experience other types of evidence, such as paper evidence, can easily be destroyed.

3.5.3 Management of electronic evidence

The last distinction relates to the storage of information. Silvernail (1997:176-177) mentions that the existence of computers has changed the way information is stored as well

as the means of communication. The researcher notes that, for example, 10 boxes of paper documents require more storage space than the same set of documents stored in electronic format on a computer. The transfer of information stored in boxes will require time, money and labour to transport from one location to another while the information stored in a computer can be transferred all over the world in far less time. Stippich (2006:3) confirms that electronic information is easy to manage compared to paper documents, which are labour intensive to manage. Hrycko (2007:3) also mentions that for paper documents more time and quite complex methods may be required to search for particular information, while standard office computers could search all of the documents for precise information in far less time.

3.6 Summary

It has been established in this chapter that electronic evidence just like any other type of evidence can be used to prove facts and assist the court to reach a conclusion about the guilt or innocence of a suspect. The audit trails left on the computer can be used to link a suspect to a crime. The central distinction between electronic and paper evidence is that, even though when information is deleted from the computer, on the surface one can assume that it is deleted, however based on how information is stored on a computer, at best this can make it harder to totally delete unwanted electronic evidence. In contrast, when a paper document is destroyed either by shredding or using other destructive means to dispose of information, that document will be completely destroyed and is not possible to be recovered.

It has also been established that the South African courts find it difficult to classify electronic evidence. There is confusion amongst the courts about whether to treat electronic evidence as real or documentary evidence. This is because electronic versions of documents are used as evidence to substantiate computer fraud.

In the next chapter the researcher focuses on the methods that can be used to collect electronic evidence.

CHAPTER 4
COLLECTION OF ELECTRONIC EVIDENCE

4.1 Introduction

Cross (2008:30) indicates that the investigation and collection of electronic evidence from the computer remain the primary responsibility of law enforcement. Cardwell *et al.* (2007:12) explain that investigators obtain such electronic evidence in order to link a suspect to a crime. According to Bryant (2008:50), the collected electronic evidence is used in investigations to support an enquiry and a subsequent prosecution. It is therefore of great importance, as mentioned by Stephenson (2000:88), that the evidence be collected properly and legally because if it is not it will be excluded as evidence in court. This then, as suggested by Bryant (2008:70), calls for an investigator with specialist knowledge in handling electronic evidence to use well-established investigative techniques to collect such evidence.

This chapter starts with a discussion on the investigation and collection of electronic evidence. This in turn leads to a discussion on the importance of maintaining a chain of custody. The researcher also discusses the importance of obtaining a search warrant for purposes of collecting evidence and the procedure for obtaining such a warrant. The chapter concludes with a discussion on how experts can assist in the collection, preservation, analysis and presentation of electronic evidence.

4.2 Electronic evidence collection process

According to Lentini and Lentini (2006:115), an investigator should always have a plan on how evidence that supports an investigation will be collected. This necessitates that the investigator knows where to search for electronic evidence and what to look for (Kipper, 2007:58). Gahtan (1999:31) mentions that the investigator needs to determine what computer systems and what software applications on these systems may contain electronic evidence. However, Lange and Nimsger (2004:23) explain that the difficulty in trying to find and retrieve electronic evidence is that there are many and complex storage locations in a computer system.

According to Vacca (2005:224), the established general forensic procedures to be followed in investigating electronic evidence include but are not limited to identification, preservation, acquisition, authentication and analysis. The researcher has observed that the collection of electronic evidence is one of the phases in the investigation process and is often referred to as the 'acquisition stage'. It is therefore also important to elaborate on the other phases of the general forensic processes relating to the investigation and to discuss the collection of electronic evidence as part of this process.

4.2.1 Identification of possible sources of evidence

According to Hrycko (2007:143), the first phase in the collection of electronic evidence starts with identifying the potential sources of such evidence. The known sources of electronic evidence, as mentioned by Velasco (2007:6), can include the following places:

- "Electronic mail or instant messages;
- Internet/intranet files;
- Temporary or recycle bin folders;
- Times of user creation, access, or deletion and
- Server and gateway log files."

In general, as noted by Philipp, Cowen and Davis (2009:16), data can be located anywhere, from personal computers to company servers. According to Anson and Bunting (2007:11), a computer crime scene can be loaded with potential evidence and the investigator should identify the sources of evidence by performing the following:

- "Determine the topology and normal usage of the network;
- Speak to the system administrators;
- Examine logs of impacted and related systems and
- Examine output from Intrusion Detection System (IDS) and other network security devices."

Once the location of the relevant evidence is identified, as indicated by Lange and Nimsger (2004:89), such evidence must then be retrieved. For this purpose the understanding of potential sources of electronic evidence (Christopher, 2007:47) will assist the investigator to preserve the potential evidence.

4.2.2 Preservation of electronic evidence

According to Pearlstein (2002:998), the duty to preserve electronic evidence arises as soon as the investigator has identified the evidence. Vacca (2005:224) indicates that it is important to preserve the collected evidence in as close to its original state as possible. In order to ensure proper preservation of evidence, the Best Practices for Seizing Electronic Evidence: A Pocket Guide for First Responder (2006:3-6) by the United States Secret Service advises that the procedures below be followed in the order in which they are set out here:

- "Do not use computer or attempt to search for evidence;
- Photograph computer front and back as well as cords and connected devices, as found;
- Photograph surrounding area prior to moving any evidence;
- If computer is "off", do not turn "on";
- If computer is "on" and something is displayed on the monitor, photograph the screen;
- If computer is "on" and the screen is blank, move mouse or press space bar (this will display the active image on the screen). After image appears, photograph the screen;
- Unplug power cord from back of tower;
- Diagram and label cords to later identify connected devices;
- Disconnect all cords and devices from tower;
- Package components and transport / store components as fragile cargo;
- Seize additional storage media;
- Keep all media, including tower, away from magnets, radio transmitters and other potentially damaging elements;
- Collect instruction manuals, documentation and notes;
- Document all steps involved in the seizure of a computer and components;
- If the computer is on a network server, consult a computer specialist for further assistance and
- Secure the scene and do not let anyone touch except personnel trained to handle network systems."

The reason for preserving the collected evidence in as close to its original state as possible, as mentioned by Crayton (2003:222), is that any potential evidence will not be admissible

in a court of law if it is corrupted, damaged or not handled with due care. This is often a challenge with electronic evidence, as explained by Feigenson and Dunn (2003:109-110), because on the surface this type of evidence is easy to forge, alter, delete or modify. It is therefore critical, as suggested by Anson and Bunting (2007:8), that the investigator collect electronic evidence promptly and correctly.

4.2.3 Electronic evidence collection

Cross (2008:210) explains that 'acquisition' refers to the process of collecting electronic evidence from the computer system. Bryant (2008:60) states further that 'acquisition' is the stage where evidence is copied from the computer and preserved in its original form. Kanellis (2006:58) emphasises that the identified evidence should be captured correctly so that it cannot lose integrity and value and as a result be inadmissible in court. Kanellis (2006:273) further mentions that securing and collecting electronic evidence with proper care is a general forensic and procedural principle that should always be applied. It is therefore critical, as indicated by Cross (2008:211), for investigators to ensure that electronic evidence remains secured throughout the investigation. For this reason (Anson & Bunting, 2007:11), evidence must be collected in a way that preserves its value in a criminal proceeding. Failure to handle evidence properly, as cautioned by Kovacich and Jones (2006:137), will render it inadmissible as evidence in legal proceedings.

With regard to the collection of evidence, the 25 participants and five expert participants provided varying responses to the question "What are the standards or legal requirements for collecting and preserving electronic evidence?" The first section of reporting deals with the 25 participants and the second one with the five experts. From the responses provided by the 25 participants, two participants suggested that each department or organisation should have an appropriate policy that conforms to international standards for collecting electronic evidence. 12 participants mentioned that the existing standard operating procedures on investigation and evidence collection in their department serve as guidance for investigators in collecting electronic evidence. Three participants said that it would be better if standard operating procedures are designed to deal specifically with electronic evidence because the existing standards are too generic and this makes the investigators' work difficult. Six participants said that the police are assisting in collecting and preserving electronic evidence and it should be a standard requirement for each organisation that a

skilled and properly trained investigator or an expert be the only one authorised to collect electronic evidence. Four out of the 25 participants said they were not sure.

The five expert participants provided the following responses; three participants indicated that in South Africa there are no procedures on the collection of electronic evidence that have been tested by courts. This statement confirms the view of Hofman (2006:30) who reports that the South African law of electronic evidence namely; the Electronic Communications and Transactions Act 25 of 2002 will only be fully effective if the courts can approve detailed procedures in conformity with the general law and the Constitution for the collection, preservation and presentation of electronic evidence in courts. One participant indicated that the International Criminal Police Organization (INTERPOL) has set standards on the collection, preservation, analysis and presentation of electronic evidence. Another participant confirmed this and added that the INTERPOL standards can be customised to form standard operating procedures that suit the situation of each organisation and that these international standards are applied by the South African law enforcement. From this, the researcher was able to deduce that these international standards have not been tailored into standard operating procedures aligned to the Electronic Communications and Transactions Act 25 of 2002.

These international standards relating to the collection, analysis and presentation of electronic evidence as referred to by the expert participants were, according to Mohay, Anderson, Collie, De Vel and McKemmish (2003:123), drafted in 1997 by the Association of Chief Police Offices (ACPO) of England, Wales and Northern Ireland and were entitled "Best Practices Guide for Computer Based Evidence". In 1998, as mentioned by these authors, the United States (US) established a working group that was assigned to craft cross-disciplinary guidelines and standards for the collection, analysis, preservation, and presentation of electronic evidence.

Marcella and Greenfield (2002:165) mention that the working group was known as the 'Scientific Working Group on Digital Evidence' (SWGDE) and that the group proposed that standards for collaboration on electronic evidence amongst sovereign nations be created. According to the authors, both the United Kingdom (UK) and US working groups were components of the efforts towards uniformity in handling electronic evidence

conducted by the International Organization on Computer Evidence (IOCE), which comprised working groups in Canada, Europe, the UK, and the US.

According to Mohay *et al.* (2003:123), the United Kingdom good practice guide and the SWGDE draft standards were reviewed in meetings and a workshop held by the IOCE during the International Hi-Tech Crime and Forensics Conference (IHCFC) in October 1999. A set of principles were presented and approved at that conference. These principles were also formalised in 2001 at the 13th International Criminal Police Organization (INTERPOL) Forensic Science Symposium and are outlined by Pollitt (2001:102) as follows:

- "Upon seizing digital evidence, actions taken should not change that evidence;
- When it is necessary for a person to access original digital evidence, that person should be competent;
- All activities relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review;
- An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession and
- Any agency which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles."

The response by some out of the 25 participants is an indication that the participants appear to have limited knowledge of the required standards for the collection of electronic evidence. An explanation for this might be that they have not been properly trained regarding procedures and expertise in collecting electronic evidence. Hence, more than one participant (investigators) mentioned that they rely on police officials to collect electronic evidence. This is an indication that the participants are not even aware of the existence of international principles such as those developed by INTERPOL, as mentioned by the some of the expert participants. The assertion by Kennedy (2004:1) that there are no established standards, regulations or procedures for the handling of electronic evidence do not hold because the existence of international standards in this regard has been proven, as discussed above. Hatch (2008:567) is of the opinion that the general procedural standards used in criminal and civil cases can be extended to electronic evidence. This is doubtful because the traditional methods as indicated by the expert participant from an institution of higher

learning have not proved useful in the collection of electronic evidence and, thus, a different technique must be implemented.

In light of the previously mentioned international standards, it is clear, as noted by Gahtan (1999:22), that the investigator needs to take precautions not to alter the original evidence in the process of copying evidence from the computer system. For this reason the investigator must maintain a backup of information obtained during collection, in case it happens that the computer system fails (Nelson, Olson & Simek, 2006:20). Clearly, as pointed out by Carmichael, Whittington and Graham (2007:487), the details of the collection process and any information about the computer from which the evidence was collected, for example, serial numbers of the computer or hard drives, should be recorded. Upon completion of the collection phase, the investigator will then focus on authenticating the collected evidence.

4.2.4 Authentication of electronic evidence

According to Cross (2008:210), authentication involves validation of evidence extracted from a computer system to ensure that it is as legitimate as the original. As articulated by Mason (2006:11), authentication relates to the question of whether the document is what it claims to be.

Mason (2006:11) explains that an adjudicator will be required to determine the credibility or reliability of the evidence presented and tested in court. As pointed out by Kanellis (2006:60), this emphasises the fact that the investigator must be able to convince the court that the evidence was derived from the computer in the crime scene. For instance the investigator may use information about security access to the computer files as proof that the evidence has not been tampered with whilst in the computer system, as mentioned by Banks (2002:159). Once the evidence has been authenticated, it is necessary that the investigator perform an analysis of the collected evidence.

4.2.5 Analysis of electronic evidence

According to Kleiman (2007:192), analysis is the process of examining and evaluating information. Lange and Nimsger (2004:92) explain that during this process the investigator examines the history of the information; for example, who edited or accessed the information, and determines whether electronic evidence was tampered with. Another point

of great importance, as noted by Cardwell *et al.* (2007:10), is that a duplicate copy should be used for analysis in order to preserve the original evidence.

Anson and Bunting (2007:13) caution that when analysing evidence the investigator should always keep in mind that the process can lead to uncovering sources of new evidence. This supports Lange and Nimsger (2004:92) view that the amount of information recoverable through the analysis process may have endless results by leading to new information.

In light of the above, Kanellis (2006:60) enlightens us that the investigator may consider using special analysis tools to analyse the evidence seized. These tools help with the visualisation of the evidence in a form of flow and link analysis charts, as observed by Casey (2004:185). The views of the 25 participants and the five expert participants in answering the question "Can information that has been interpreted through the use of a software tool be accepted as evidence at trial?" are reported in two parts. The first section of reporting deals with the 25 participants and the second one deals with the five experts. From the responses provided by the 25 participants, 12 participants said that if it is good evidence then it will be admissible. Three participants said that the information can only be used to assist prosecution in visualising the evidence. Two participants said that it is up to the investigator to decide whether or not to present the evidence in court and three participants said that the judge will decide if it can be used or not. Five out of the 25 participants said they did not have any idea about the answer and were not aware of such a tool.

In answering the same question, the five expert participants provided informative views. One participant said that, when such information is used as evidence, the tool used to interpret the evidence must meet the standards of information technology-related evidence. Two participants said that the product can be admitted as evidence in court if the investigator can convince the court that if an independent party were asked to analyse the evidence they would also be in a position to produce related result and come to the same conclusion. Two participants diverged from this view and said that the product only assists the prosecution in the interpretation of the data and also in providing a broader picture about the evidence up for presentation. Mohay, *et al*. (2003:133) affirm that the evidence presented through these mediums can only assist in providing an understanding of relationships and therefore cannot be used as a substitute for the actual evidence.

The response from the majority of the 25 participants is an indication that they do not have knowledge of the tools that can be used to interpret information. A deduction can be made on the basis of their responses that they do not make use of the analysis software tools that are available in their working environment. This certainly has a potentially negative impact on an investigation because a great deal of information might be missed during the analysis process.

4.2.5.1 Analysis of encrypted evidence

Encryption is the use of digital artifact to transform readable information to an unreadable format (Craiger, Swauger, Marberry 2005:1). From experience the researcher detected that criminals encrypt information to hide evidence. According to Casey (2002:6-7) encryption applications have flaws that can be taken advantage of to recover some or all encrypted data. The author explains that at a certain stage prior to data being encrypted, it exists in unencrypted form and the plaintext might be stored temporarily in a pagefile system or stored temporarily on disk. With reference to how information is stored in the computer as previously explained by the expert participants, there is good possibility that it can be recovered through various means such as searching unallocated space on the hard drive

According to Casey (2002:6-7) even though the original documents were wiped, fragments of the files remain scattered in the disk in deleted MS Word temporary files, a quantity of which could be located by searching for Microsoft Word headers. Another method used to break encryption as mentioned by Craiger, Swauger and Marberry (2005:3) is to recover passwords (passphrase) used for encryption. According to these authors the suspect can be persuaded to provide the passphrase and if not, then passwords cracking software tools can be used.

With regard to the investigation of electronic evidence it can be concluded that, as pointed out by Anson and Bunting (2007:11), investigators should ensure that they do not alter electronic evidence during collection and that they maintain an accurate chain of custody.

4.3 Chain of custody

A chain of custody is an important principle in investigation and concerns the handling of evidence and its integrity (Marcella, Marcella-Jr & Menendez, 2007:12). The party leading the evidence in court, as indicated by Duerr, Beser and Staisiunas (2004:1), must prove the

location, date, and time of collection and demonstrate that the evidence has not been altered since collection. A chain of custody is therefore considered necessary to demonstrate the admissibility of evidence (Bergman & Berman-Barrett, 2008:400).

Schetina, Green and Carlson (2002:351) state that the admissibility of electronic evidence at trial might depend on whether the chain of custody has not been altered. Smith, Grabosky and Urbas (2004:81) caution that, in court, the defence capitalises on challenging the integrity of evidence. According to the authors, the interest of the defence is in raising doubts and confusion about the evidence assembled and presented in court by the prosecution. This is confirmed by Casey (2004:184), who mentions that during cross-examination the attorneys make an effort to expose any flaws and facts that were disregarded by the investigator. Caloyannides (2004:313) explains that technical details such as how a chain of custody was maintained during the collection of electronic evidence can determine whether an investigator will win or lose a case.

The five expert participants were asked the question “What information should be documented as proof that a chain of custody was maintained in handling evidence?” One of the participants from an institution of higher learning indicated that the particulars of the persons who collected the electronic evidence should be documented. The other three of the five participants pointed out that details of the procedures used to collect the evidence, for example, the tools used and the people performing the procedure, must be documented. The remaining participant said that a list of all media that were secured and the exact information that was collected must also be documented. In addition all participants listed the details that should be documented in the chain of custody as including “date, time and place where the evidence was collected”, “details of custodians and the manner in which the electronic evidence was transferred to subsequent custodians”, “security conditions relating to the handling or storage of the electronic evidence” and “details on how the analysis was performed”.

From the above it is clear, as indicated by Lange and Nimsger (2004:76), that the court will need to be informed about the steps taken to ensure that the electronic evidence was not tampered with. Kanellis (2006:59) emphasises the fact that the investigator must maintain a clear chain of custody to protect the integrity of the evidence and should be able to demonstrate that the electronic evidence is trustworthy. Equally important, Van der Merwe,

Roos, Pistorius and Eiselen (2008:85) explain that the prosecution will have to convince the court that the evidence has not been interfered with from the time of seizure to the time it was presented in court. As mentioned by Stephenson (2000:133), this will then put the prosecutor presenting evidence at an advantage in proving to the court that the electronic evidence was protected from alteration.

To determine the importance of maintaining a chain of custody to the sample of the study, the 25 participants and the five expert participants in this study were asked the question "Why is it important to maintain a chain of custody when collecting and preserving electronic evidence?" The first section of reporting deals with the 25 participants and the second one with the five experts. From the responses provided by the 25 participants, 16 participants said that it helps to ensure that the evidence does not get manipulated and that it remains authentic. Nine out of the 25 participants were too general in their responses and said "because it is important", "it is necessary" and that "it is expected that a good investigator should maintain a chain of custody".

As mentioned earlier, the five expert participants were also asked he same question. One participant pointed out that maintaining a chain of custody ensures accountability and that if this accountability cannot be maintained such evidence can be inadmissible in court. Two participants said that maintaining a chain of custody enables one to track the movement of evidence from when evidence is seized to when it is presented in court as that evidence exchanges hands. The other two participants indicated that investigators maintain a chain of custody to preserve evidence properly. According to one of the participant, maintaining a chain of custody assures the integrity of the evidence.

From the responses provided by the expert participants, it is evident that a chain of custody validates the integrity of evidence, which is critical for its admissibility at trial. It is clear that a lack of knowledge by some of the 25 participants on the importance of maintaining a chain of custody can have a negative impact on the outcome of cases. From the researcher's experience it is clear that if an investigator cannot prove that the evidence presented before the court is trustworthy, such evidence will be regarded by the court as inadmissible. This is an indication that proper training on the collection of electronic evidence is a necessity.

Another point of great importance in preserving a chain of custody, as indicated by Jacko, Stephanidis and Harris (2003:705), is that the investigator must always operate within the law enforcement best practices, for example by obtaining a search warrant and following set guidelines to seize computers and acquire electronic evidence. For this reason the procedure to follow in obtaining a search warrant is discussed in the section below.

4.4 Obtaining a search warrant

Cross (2008:216) defines a search warrant as a legal document that authorises only law enforcement officers to search for and seize evidence related to an investigation which may possibly be used in court. A search warrant is issued in terms of section 21 of the Criminal Procedure Act 51 of 1977 and this section provides certain formal requirements which are not discussed here, that a search warrant has to comply with.

On the basis of her experience the researcher has learnt that a law enforcement officer may present a written application in the form of a sworn affidavit to a magistrate in order to obtain a search warrant. The only people that can apply for a search warrant as per the provisions of section 43(1) of the Criminal Procedure Act 51 of 1977 are a commissioned officer in the South African Police Service, a director of public prosecution and a public prosecutor (South Africa, 1977:sec.43(1)). The same section further stipulates that a magistrate and a justice of the peace are the only people that may issue a warrant.

According to Joubert (2001:237), the application for a warrant must be in writing and should provide the following information:

- "a description of the crime alleged to have been committed;
- that the crime was committed within the area of jurisdiction where the application is made and if not, then the suspect is known to be within the area of jurisdiction and
- that there is a reasonable ground that the suspect has committed the crime based on information obtained under oath."

It is important to provide the above mentioned information because, according to section 14 of the Constitution of South Africa 108 of 1996, a person has a right not to have their person, home or property searched or their possessions seized (South Africa, 1996:sec.14). To ensure that people's privacy remains protected, an investigator is required to provide

proof that it is necessary to conduct a search and to seize a person's property before the court can authorise such a warrant (Stephenson, 2000:88). In addition, Sterneckert (2003:362) mentions that it is crucial for the search warrant to be specific about the area to be searched as well as the evidence to be seized.

In cases that involve computers, Casey (2004:215) advises that the investigator must first conduct research and get sufficient information about the search site, the computer equipment to be expected and the sources of electronic evidence, so to cover all the details in the search warrant. This supports the view of Kovacich and Boni (2000:247) who mention that the investigator will be better prepared to conduct an effective search if sufficient information about the location to be searched is obtained prior to conducting the search.

Sterneckert (2003:362) cautions that an investigator can only search and seize within the scope of a warrant. In *Minister of Safety and Security v Bennett* 2007 SCA 139 (RSA), the police seized privileged documents which were not authorised by the search warrant and the court ordered for the return of the documents to the applicants. Sterneckert (2003:362) further advises that after the initial search the investigator should obtain another search warrant to collect any other newly identified evidence at the crime scene not covered in the warrant under execution.

The researcher has observed that there are certain documents or information whose seizure cannot be authorised by the courts even when an application for a new warrant is made for their seizure. The attorney-client privilege information documents in *Minister of Safety and Security v Bennett* 2007 SCA 139 (RSA) are an example of documents for which a court will not authorise a warrant for seizure. In addition, as mentioned by Van der Merwe and Du Plessis (2004:519), a police official can only search and seize without a warrant under the following conditions:

- "when consent is granted by the person in charge of the goods or premises
- where an investigator believes on reasonable grounds that a warrant would have been issued and that any delay to obtain one would defeat the objectives of the search."

The search conducted by the police in *Mabona v Minister of Law and Order* 1988 (2) SA 654 SE at 660 D was found to be reasonable and based on the need for immediate effective police action to investigate the information with which the investigators had been furnished. The court held that if swift and effective action was not taken, the suspects might be forewarned and evidence might disappear. The evidence was admitted by the court in this regard. In *Key v Attorney-General, Cape Provincial Division* 1996 (6) BCLR 788 (CC), the court also stated that "there will be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted".

Wrongful search is an offence under section 28 of the Criminal Procedure Act 51 of 1977, and any person who has suffered damage as a result of an unlawful search or seizure may approach the court and be awarded compensation in respect of such damage. In *Minister of Safety and Security v Liddell* 2002 (247/2001) ZAECHC 5, the respondent was awarded damages in the sum of R20 000-00 for wrongful search, arrest, detention, assault, and injury to his dignity and reputation.

4.5 The utilisation of experts

Christopher (2007:26) defines an expert in any field as "one who has special knowledge, skill, experience, training or education in a particular field". The researcher also believes that almost all professions require a level of specialisation to carry out certain responsibilities. For instance, a data capturer needs typing skills in order to capture information at a speed required to perform a certain task. Similarly, in computer forensics only a computer forensic expert will be in a position to retrieve information hidden in a computer hard drive, especially in cases where it might appear as if the information has been completely damaged or lost, as explained by Pollitt (2001:100).

Stephenson (2000:13) mentions that investigators in other organizations mandated by legislation to conduct investigations outside the police service are not skilled and lack in-depth technical knowledge for investigating computer crimes. Barbara (2008:12) suggests that investigators should be properly skilled in the collection and preservation of electronic evidence. If, as mentioned by Jacko *et al.* (2003:704), investigators are not properly trained in the legal requirements for handling electronic evidence, such evidence cannot be used at trial. The assistance of a skilled computer forensics expert can therefore be important in

collecting electronic evidence where investigators are not well equipped to do so, as recommended by Overly (1999:2).

To determine the importance of using an expert in the collection of electronic evidence for the sample of the study, the 25 participants and five expert participants were asked the question "Why should computer forensic experts be used in collecting electronic evidence?" The first section of reporting deals with the 25 participants and the second one deal with the five experts. From the responses provided by the 25 participants, four participants pointed out that experts can assist in resolving challenging computer software or hard drive issues that arise in the collection of electronic evidence. Three participants indicated that experts can assist in finding and examining important computer information that can be used as evidence at trial. 18 out of the 25 participants reported that experts are more knowledgeable than ordinary employees because they are adequately trained to handle electronic evidence. The participants appeared to be familiar with the reasons for using computer forensic experts to collect, preserve, analyse and present electronic evidence in court.

The knowledge of the five expert participants were also tested on the same question as previously noted. Four participants pointed out that electronic evidence expert are skilled in recovering incriminatory information from computer hard drives even when such information has been deleted by the suspect. One participant explained that computer forensics is unquestionably a highly specialised field and that as a result not everyone is skilled enough to handle electronic evidence and produce high quality evidence. The fact that not all investigators are skilled enough to handle electronic evidence as mentioned by the expert participants is an indication that with in-depth training their skills could be further developed in the collection and preservation of electronic evidence.

4.6 Summary

It has been established that in South Africa there are no adopted standard processes for the collection, preservation and analysis of electronic evidence that have been developed and tested in court. The laws regulating electronic evidence will only be fully effective if such processes can be established and implemented. It is however, noted that investigators must maintain a chain of custody by always ensuring that electronic evidence is collected, preserved and analysed in a manner that will ensure its admissibility in court. The chain of

custody assures continuous accountability. The starting point of cases relating to electronic evidence is to handle the evidence properly. The assistance of a skilled computer forensics expert can therefore be important in collecting electronic evidence where investigators are not well equipped to do so.

The above discussion deals only with the phase of electronic evidence collection. The second equally important phase is presenting the electronic evidence in a court of law as evidence against a suspected criminal to secure a successful conviction. For this reason, the next chapter is used to discuss the legal requirements for admissibility of electronic evidence.

CHAPTER 5

LEGAL REQUIREMENTS FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE

5.1 Introduction

According to the Oxford Advanced Learner's Dictionary (1989:16), 'admissibility' can be defined as "worthy of being accepted or considered". Kanellis (2006:284) explains that any kind of evidence assumes two elements: firstly, the formal requirements that are contained in legislation, which refer to its admissibility under the law; and, secondly, the material requirements, which focus on the credibility of evidence presented in a case.

With regard to the above, Bryant (2008:52) cautions that presenting electronic evidence in court has challenges. This is because electronic evidence is information that can be easily manipulated and distorted and therefore, as mentioned by Marcella *et al.* (2007:282), it will always have to be subjected to serious legal scrutiny. Jacko *et al.* (2003:704) caution that courts adhere to high standards of proof when it comes to presenting evidence in court. As mentioned by Hatch (2008:567), the legality and reliability of evidence are some of the essential requirements that will be considered by the judiciary when deciding on the admissibility of evidence.

In this chapter the researcher begins by discussing the South African legal framework on electronic evidence. This is followed by a detailed discussion about the requirements for admissibility of electronic evidence, which leads into a brief discussion on hearsay evidence. The chapter concludes by explaining the role of the investigator in presenting electronic evidence in court and the challenges brought about by electronic evidence in court.

5.2 South African legal framework for electronic evidence

A provision for admissibility issues relating to computer printouts was not made in the Civil Proceedings Evidence Act 25 of 1965. The Computer Evidence Act 57 of 1983 was therefore enacted to address the criteria for the admissibility of computer evidence in civil cases. It was a requirement under the Computer Evidence Act 57 of 1983 to have an affidavit accompanying all evidence presented in court. The purpose of the affidavit was to

verify the identification of a printout, sources of the evidence, and certification that the computer from which the printout was made was in good working order. A huge burden of proof was placed on the experts presenting computer evidence by this Act.

The Computer Evidence Act 57 of 1983 was furthermore only applicable to civil proceedings and therefore, as observed by the researcher, criminal proceedings were not regulated. The South African Law Commission Project (1995:iv) recommended that the Computer Evidence Act 57 of 1983 be repealed. The Law Commission proposed that the Criminal Procedure Act 51 of 1977 and the Civil Proceedings Evidence Act 25 of 1965 be modified to make provision for computers and computer printouts. The Criminal Procedure Act 51 of 1977 as a result expanded the term "document" to include electronic information. In addition to this, the Electronic Communication and Transactions Act 25 of 2002(a) has since been passed and this Act regulates matters regarding the use of electronic evidence in both criminal and civil proceedings.

With regard to the legal framework on electronic evidence, the 25 participants and five expert participants were asked the question "Which legislation can be relied on for admissibility of electronic evidence?" The first section of reporting deals with the 25 participants and the second one with the five experts. From the responses provided by the 25 participants, 11 participants mentioned the Electronic Communication and Transactions Act 25 of 2002(a). Six participants listed the "Criminal Procedure Act 51 of 1977" and the "Electronic Evidence Act". Eight out of the 25 participants said they did not have an idea.

When responding to the same question the five expert participants listed the "Electronic Communication and Transactions Act 25 of 2002(a)", "Criminal Procedure Act 51 of 1977", "Promotion of Access to Information Act No 2 of 2000" and the "Constitution of the Republic of South Africa No. 108 of 1996(a)". One of the participants mentioned the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002(c). In addition to these responses another participant mentioned the Copyright Act, No. 2 of 1959 and the Protection of Personal Information Bill also known as the 'Data Privacy Bill'.

The majority of the 25 participants lacked knowledge concerning the legal framework on electronic evidence. The lack of knowledge by the participants regarding the legal

framework on electronic evidence is likely to have a negative impact on investigations and the collection, preservation, analysis and presentation of evidence, as it may result in evidence collected being rendered inadmissible by the courts because it does not meet the requirements for admissibility of evidence.

According to all the expert participants, the Electronic Communication and Transactions Act 25 of 2002(a) is the most important legislation dealing with electronic evidence. This view is confirmed by Van der Merwe *et al.* (2008:75), who mention that the criminal provisions in the Electronic Communication and Transactions Act 25 of 2002(a) "so far, are the mainly significant legislative countermeasures against computer crimes in South Africa". According to these above mentioned authors, the Electronic Communication and Transactions Act 25 of 2002(a) deals with the presentation of electronic information and can be used in conjunction with the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002(c), which deals with the collection, preservation and reporting of electronic information.

Section 15 of the Electronic Communication and Transactions Act 25 of 2002(a) deals with electronic evidence and provides two grounds on which data messages may not be denied admissibility. Section 15 reads as follows:

> "Admissibility and evidential weight of data messages -
>
> 1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data messages, in evidence
>
> a) on the mere grounds that it is constituted by a data message; or
>
> b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form."

Section 15 of the Electronic Communication and Transactions Act 25 of 2002(a), as mentioned by Hofman (2006:3), is based on the model law and as such is in conformity with international standards. The aim of the model law, as mentioned by Thornton, Carrim, Mtshaulana and Reburn (2006:264), is to provide national legislatures with a guide of internationally acceptable set of laws to create a more secure legal environment for electronic commerce.

5.3 Electronic evidence and the rules of evidence

MacNeil (2000:50) states that traditional rules of evidence have remained applicable to electronic evidence. Schmidt and Rademeyer (2006:11) are also of the same opinion, as they mention that the ordinary rules of evidence apply to electronically produced data. Nevertheless, the South African ordinary rules of evidence have been refined by the provisions of the Electronic Communication and Transactions Act 25 of 2002(a) with regard to electronic evidence, as mentioned in the Strategic Value of Electronic Discovery (2007:1).

Hofman (2006:7) explains that the Electronic Communication and Transactions Act 25 of 2002(a) only regulates electronic information and does not as a result reform the law of evidence. This therefore implies that the South African law of evidence is still applicable to electronic evidence, except where it is changed by the Electronic Communication and Transactions Act 25 of 2002(a).

5.4 Requirements for admissibility of electronic evidence

Francoeur (2003:3) explains that admissibility relates to the requirements necessary to hold an individual accountable, to obtain a successful dispute resolution ruling, or to secure positive court adjudication. Accordingly, the admissibility of any evidence whether adduced orally or electronically must have an adequate level of relevance to a matter in issue, as mentioned by Laryea (2003:11). However, any relevant evidence which might appear to be problematic may still be excluded by the South African courts, as cautioned by Zeffert, Paizes and St Q Skeen (2003:219). This is illustrated *in R v Schaube-Kuffer* 1969 2 SA 40 (RA), where it was held that evidence that is reliable and relevant to the facts in issue is admissible unless it is prohibited by the exclusionary rule.

Hrycko (2007:167) indicates that electronic evidence might tend to be problematic in that it can be easily altered and that may possibly render it inadmissible in a court of law. Paper documents on the other hand, as noted by Laryea (2002:28), are readily acceptable by the courts unless there are genuine reasons for disputing their authenticity and such acceptance is lacking in electronic evidence because it is viewed with suspicion.

Schmidt and Rademeyer (2006:11-4) are of the view that electronic evidence will not be subjected to a special set of admissibility requirements. However, the admissibility of data

messages according to the Electronic Communication and Transactions Act 25 of 2002(a) must harmonise with the ordinary requirements for the admissibility of documents in the South African law of evidence.

With regard to the above, the 25 participants and five expert participants were asked the question "What are the legal requirements for admissibility of electronic evidence?" The first section of reporting deals with the 25 participants and the second one with the five experts. From the responses provided by the 25 participants, seven participants pointed out that the evidence must have been properly collected. Five participants said the evidence must be original. Four participants indicated that the evidence must be presented properly. Three participants said that there must be proper investigation and consultation with other stakeholders. Six out of the 25 participants said that they did not have an idea.

In response to the same question, three of the five expert participants reported that the investigator must demonstrate to the court that the document retrieved from the computer is the same as the original record in the computer. Two participants explained that the investigator must convince the court that the electronic evidence is reliable, authentic and original. This supports the view of Hofman (2006:7) who states that the ordinary requirements for the admissibility of documents, which electronic evidence must satisfy, are that the documents must be reliable, authentic and original. The views these two participants furthermore also support Hatch (2008:567), who states that some fundamental requirements that might be considered by the court in deciding on the admissibility of evidence are:

- "Originality of evidence;
- Reliability of evidence;
- Authenticity of evidence;
- Legality of evidence and
- Is it the best evidence available?"

In addition one of these expert participants pointed out that the computer system in which the evidence was stored and from which it was retrieved must be one of integrity. Another participant said that the investigator must convince the court that the electronic evidence is the best evidence available to be presented in court.

The majority of the 25 participants could not provide appropriate answers on the legal requirements for admissibility of electronic evidence at trial which are relevance, reliability, and authenticity. In general, the above are the legal requirements that electronic evidence must satisfy to be admissible in court. The following sections elaborate further on the specific legal requirements for admissibility of electronic evidence.

5.4.1 Production of electronic evidence

According to Hofman (2006:7), a document must first be produced for it to be eligible as evidence. Vere (2009:8) explains that weight is generally attached to production of the original document when it comes to paper-based evidence. However, the problem with electronic evidence is that it can be altered with relative ease, according to Tipton and Krause (2003:826). Hrycko (2007:177) warns that this can create problems with the admissibility of such evidence at trial.

Zondo-Kabini (2003:78) points out that the Electronic Communication and Transactions Act 25 of 2002(a) gives computer-generated documents the same legal status as traditional paper evidence. In *S v Harper* 1981 (1) SA 88 D, the court held that computer printouts are regarded as documents. The definition of a document in section 221(5) of the Criminal Procedure Act 51 of 1977 also includes a device through which information is stored and recorded (South Africa, 1977:sec.221(5)).

Section 17 of the Electronic Communication and Transactions Act 25 of 2002(a) permits a person who is required by law to produce a document or information (South Africa, 2002:sec.17). The requirement is met if such information is produced electronically provided that it meets certain requirements, including its integrity. Zondo-Kabini (2003:1) mentions that a copy of a data message certified to be correct by an officer in the service of a person or a data message made by that person in the ordinary course of business will on mere production in any proceedings under any law be admissible in evidence against that person.

5.4.2 Original form

Secondly, it is a requirement of the rules of evidence as indicated by Zeffert *et al.* (2003:686) that when the document is made available as evidence it must be an original.

Although this may be a requirement, it is subject to certain exceptions as pointed out by the authors. The court held in *Barclays Western Bank Ltd v Creser* (2) SA 104 (T) 106 that no evidence is ordinarily admissible to prove the contents of a document except the original document itself. However, data messages are exempted from this ruling under section 15(1)(b) of the Electronic Communication and Transactions Act 25 of 2002(a), which makes a provision for their admissibility and states that a data message is admissible even though not in its original form provided that it is the best evidence available (South Africa, 2002:sec.15(1)(b)).

According to Hofman (2006:7), section 17 of the Electronic Communication and Transactions Act 25 of 2002(a) makes a provision for the production of a document in the form of a data message provided it meets the requirements in the section on ensuring that the document is trustworthy. The Namibian court held in *S v De Villiers* 1993 (1) SACR 574 (Nm) that a computer printout is a duplicate original and therefore admissible provided it is certified as authentic. Equally important, as explained by Thornton *et al.* (2006:271), is that a computer printout, although it can be accepted as electronic evidence, does not constitute an original. The author explains that the original message remains in electronic form in the computer system.

5.4.3 Authenticity

The third requirement for admissibility of electronic evidence is authenticity. Casey (2004:172) explains that authentication is the process of determining whether evidence is worthy. According to Galves (2000:229-230), authentication is meant to ensure that the evidence is what it purports to be. As mentioned by Hofman (2006:8), it is a requirement under the rules of evidence for a person using documents as evidence to satisfy the court that these documents are authentic. In *Moloko v Ntsoane and Others* 2004 (JR 1568/02) ZALC 35, the applicant challenged the admissibility of the unauthenticated evidence that was relied on by the respondent to dismiss the applicant from work. The court found the use of unauthenticated electronic evidence as inadmissible.

Galves and Galves (2004:3) elaborate further on the concept and state that authentication means satisfying the court that:

- “the contents of the record have remained unchanged;

- that the information in the records does in fact originate from its purported source, whether human or machine and
- that extraneous information such as the apparent date of the record is accurate."

Generally, the principles for the admissibility of evidence, as confirmed by Kenneally (2005:5), are relevance, reliability, and authenticity. According to the author, the evidence must not be hearsay unless it falls within an exception to the hearsay prohibition.

5.5 Hearsay evidence

According to Van der Merwe and Du Plessis (2004:498), hearsay is defined in section 3(4) of the Law of Evidence Amendment Act 45 of 1988(a) "as evidence whether oral or in writing, the probative value of which depends on the credibility of any person other than the person giving such evidence". Winn and Wright (2000:18) state that the purpose of hearsay is to advance the reliability and completeness of courtroom evidence.

Keena (2002:5) points out that the hearsay objection commonly takes place when electronic evidence is presented at trial. Irrespective of any objection, it is important to note that the South African law of evidence does not exclude electronic evidence if it is used for other purposes and not to prove the truth of the contents of a document, as indicated by Hofman (2006:9). As an example, in *Mdani v Allianz Insurance Ltd* 1991 (1) SA 184 (A) the court held that a statement does not amount to hearsay if it is not tendered to prove the truth of its contents. Laryea (2003:11) is in agreement and states that when electronic evidence is used to prove the existence of a fact, it is hearsay and therefore inadmissible. However, if it is tendered to prove the truth of what is contained in a statement as explained in *Estate De Wet v De Wet* 1924 CPD 341, the evidence is therefore hearsay.

According to Laryea (2003:13), electronic evidence is inadmissible under common law unless an exception applies. A variety of exceptions can be applied under s(3) of the Law of Evidence Amendment Act 45 of 1988(a), which states that hearsay is admissible on the following grounds:

- "by agreement of the party against whom the evidence is adduced;
- if the person upon whose credibility the probative value of the evidence depends testifies at the proceedings or

- if the court is of the opinion that the evidence should be admitted in the interest of justice." (South Africa, 1998(a):sec.3).

Even though hearsay evidence is admissible, based on the grounds mentioned above, according to the Public Record Office Victoria (2003:5), electronic evidence is less likely to be excluded as hearsay if it evidently falls within a scheduled, restricted and documented business process. Kaufmann-Kohler and Schultz (2004:244) indicate that electronic evidence should be regarded as admissible hearsay if it has been documented using a process that is considered legally consistent. Judge Van Zyl remarked as follows in *S v Ndiki and Others* 2008 (2) SACR 252 (Ck): "where the probative value of a statement in the print-out is dependent upon the 'credibility' of the computer itself, section 3 of the Law of Evidence Amendment Act 45 of 1988(a) will not apply."

5.6 Presentation of electronic evidence in court

Stockdale and Gresham (1995:5) mention that the most important element in the judicial decision-making process is the presentation of evidence in court. Bryant (2008:63) indicates that in the presentation stage the investigator prepares a report with details pertaining to the reconstruction of events that took place on the evidence before its seizure. Cross (2008:639) argues that the information captured in the report will depend on the case and the information retrieved from the computer system.

It is therefore important, as mentioned by Craiger, Pollitt and Swauger (2005:5), for investigators to view anything collected from a computer system as evidence that may be subject to presentation in court. Furthermore, the manner in which investigators provide evidence and their performance under cross-examination are important in determining the capability and integrity of the evidence, as explained by Stockdale and Gresham (1995:5).

To determine how electronic evidence can be presented at trial, the 25 participants and five expert participants were asked the question "How should evidence be presented at trial?" The first section of reporting deals with the 25 participants and the second one with the five experts. From the responses provided by the 25 participants, 13 participants pointed out that the investigator should be well prepared and must know the case. Four participants said in presenting evidence the investigator must focus attention on the issues. Six participants said that the presentation should be made in a way that makes it possible to understand the

evidence presented. Two out of the 25 participants pointed out that the investigator should provide all necessary information but should concentrate on the issues significant to the case. The 25 participants demonstrated a good understanding of how evidence should be presented in court.

The five expert participants were also asked the same question in this regard. Three participants advised that the investigator should always consult with the prosecution before the trial and also make sure that the facts of the case are well understood. Two participants explained that in court the investigator should start by providing background information about the case and explain all the technical terms used in computer forensics so that the court has a better understanding when evidence is presented. One of these participants further indicated that this is because electronic evidence is so technical and complex that it is beyond the technical knowledge and experience of the court.

In addition one of the expert participants emphasized that the investigator should describe to the court the procedures followed when evidence was seized and provide a detailed explanation to demonstrate those procedures that were followed. This participant also pointed out that the court is more interested in hearing that there was continuity from the time when evidence was seized to the time it was analysed at another location. Furthermore this participant mentioned that it is critical for the investigator to be able to account by showing a tracking sheet detailing the time and dates for each action performed during the handling of such evidence.

Some of the expert participants cautioned that it is critical to be well prepared; for instance, the investigator should identify and scrutinise gaps that are likely to be raised in defence. This support the view of Casey (2004:184-186), who states that preparation is essential and that the investigator would have to explain how the chain of custody was maintained during the collection, preservation and analysis of electronic evidence.

According to Mozayani and Noziglia (2006:84), the investigator must be in a better position to present the electronic evidence to the judiciary considering that the judiciary has limited knowledge not only of the processes followed in the collection, preservation and analysis of electronic evidence but also in the underlying science and technology involved in this regard.

In addition to the above, Tipton and Krause (2006:1884) indicate that successes in courts require a skilled attorney and an expert witness, all of whom can clearly explain complex technology to those who have never used a computer. This view is supported by most of the expert participants, as they mentioned that the judges are not specialists in the computing environment. The expert participants explained that an expert is better skilled to explain the evidence to the court for it to understand the evidence in a way that an ordinary person would. Another important aspect for consideration, as noted in *Goliath v Fedgen Insurance* 1994 (2) PHF 31 (E), is the fact that their opinions as experts are admissible on occasions where their special skills and knowledge make them better qualified to draw inferences than a judicial officer.

5.7 Challenges of electronic evidence in court

According to Smith *et al.* (2004:81), assembling and presenting electronic evidence at trial in a manner that is intelligible and credible is a significant challenge for the prosecution. Electronic evidence, specifically, tends to be in large volumes, as pointed out by the authors.

A challenge mentioned by Bantekas and Nash (2003:82) is the lack of training and resources. The lack of training and resources as indicated by the authors leaves investigators less equipped and without the high level of technical expertise and specialist investigative skills necessary to tackle computer crimes. This obviously means that electronic evidence is not properly identified or collected consequently leading to unsuccessful prosecutions (Greene, 2006:337). For that reason, as explained by the Technical Working Group for Electronic Crime Scene Investigation (2001:23), investigators must follow proper procedures in seizing and processing electronic evidence because that is important for making a winnable case for prosecution.

To determine the challenges faced by prosecution in dealing with electronic evidence, the 25 participants and five expert participants were asked the question: “What are the challenges faced by prosecution in dealing with electronic evidence?” The first section of reporting deals with the 25 participants and the second one with the five experts. From the responses provided by the 25 participants, 10 participants said most investigators are not properly trained in collecting, handling and presenting electronic evidence in court. Four

participants reported that not all magistrates and judges understand the technicalities of electronic evidence and as a result some cases are thrown out of court. Two participants indicated that there are no formal set guidelines for collecting, preserving and presenting electronic evidence in court. One participant said that the accused might have committed the crime in another country and it would be difficult to prosecute them in South Africa. Eight participants mentioned that electronic evidence is too complicated to understand.

The five expert participant also responded to the same question as noted above. One participant indicated that role players such as the law enforcement officers and justice officials lack training. Four participants pointed out that judges and lawyers are not specialists in computer crimes and have few or no computer skills and as a result they find it difficult to deal with cases that involve electronic evidence successfully. Tipton and Krause (2006:1884) refer to the following as significant challenges at trial:

- Few lawyers have a good enough understanding of technology to enable them to build a strong case;
- Few judges have a good enough understanding of technology to enable them to rule effectively on electronic evidence and
- The average judiciary has limited or no computer literacy.

It is clear from the views of the expert participants and the investigator participants that lack of proper training for investigators and justice officials on computer evidence has a negative impact on the outcome of cases. This confirms the view of Jacko *et al.* (2003:704) who indicate that if investigators are not properly trained in the legal requirements for handling electronic evidence such evidence cannot be used at trial. Moreover computer-related offences, as indicated by Cross (2008:655), are often poorly defined in the statutes that govern them. According to Cross (2008:655), this is because the legislators involved in making computer crime laws do not understand the technology.

Another major challenge raised by one of the 25 participants is that when computer crimes are committed across country borders it has the effect that the conduct of the accused might not be viewed as an offence and therefore might not be punishable under the laws of other countries. Similarly, another challenge identified by the Ritter (2006:21) in the prosecution

of electronic crimes is geographic boundaries. Broadhurst and Grabosky (2005:51) explain that the challenges relate to legal problems of jurisdiction and extradition, which entail:

- Determining where the offence took place and the law to be applied in that regard and
- Obtaining evidence and locating the offender to face prosecution.

According to Hedley (2006:80), the legal admissibility of electronic evidence will therefore depend on the laws of each jurisdiction. Schwikkard and Van der Merwe (2009:417) indicate that a provision is made under section 90 of the South African Electronic Communication and Transactions Act 25 of 2002(a) for extension of territorial jurisdiction in circumstances where it would not have been possible. According to the authors, this therefore addresses the challenge of jurisdiction.

5.8 Summary

The Electronic Communication and Transactions Act 25 of 2002(a) has been found to be the most relevant legislation regulating the admissibility of electronic evidence. The ordinary rules of evidence were also found to be applicable to electronic evidence; however, they are refined by the Electronic Communication and Transactions Act 25 of 2002(a) with regard to matters pertaining to electronic evidence.

It has also been established that the courts experience challenges in dealing with electronic evidence because it is a highly specialised field. Judges and lawyers are not specialists in the field of electronic evidence so they sometimes struggle to understand the technicalities relating to this type of evidence enough to enable them to rule effectively on matters involving electronic evidence.

CHAPTER 6
FINDINGS AND RECOMMENDATIONS

6.1 Introduction

This research came about as a result of the necessity to enhance the general knowledge of investigators in collecting, analysing and presenting electronic evidence at trial in order to solve crime. This research focused on investigation and the collection of electronic evidence without compromising its integrity or credibility. The focus was also on the standard or requirements for admitting electronic evidence at trial. The process of investigation requires the investigator to collect and preserve electronic evidence in a manner that is able to withstand any legal scrutiny at trial. Investigators need to be properly trained and skilled in handling electronic evidence. From experience, the researcher has observed that investigators tend to focus on traditional or document-based evidence because their knowledge in dealing with electronic evidence is limited.

The researcher is confident that this research will enhance the knowledge of investigators on the use of electronic evidence in conducting their investigations. The following research questions enabled the researcher to investigate the research problem systematically:

- What is investigation?
- What is electronic evidence?
- How can electronic evidence be collected without compromising its
- integrity or credibility at trial?
- What are the legal requirements for admissibility of electronic evidence?

The researcher is convinced that the aims and objectives of this research were achieved. The findings and recommendations below are all based on the information obtained during the interviews with investigators and experts in the field of electronic evidence, coupled with a thorough literature study on the topic.

6.2 Findings

The following findings were made on the basis of information obtained from literature and interviews.

6.2.1 Primary findings

The answers to the related research questions are discussed in the sections below.

6.2.1.1 Research question one: What is forensic investigation?

- It was established in this research that the word ‘forensic’ is derived from the Latin word *forensic*, meaning ‘giving the opportunity to debate’. In practice ‘forensic investigation’ refers to the use of science and technology to investigate events and establish facts in criminal or civil courts of law. This involves the gathering, analysis and processing of information throughout an investigation.
- 13 of the 25 participants are familiar with the concept ‘forensic investigation. 10 participants had a broad view of the meaning of investigation and two participants had a limited understanding. The response of the 10 participants who demonstrated a broad overview of this concept fell short of a comprehensive view of forensic investigation as a multidisciplinary profession since some believe that the concept has to do only with investigation of computer crimes or financial crimes. A lack of training is identified in this regard.

6.2.1.2 Research question two: What is electronic evidence?

- It was established that ‘electronic evidence’ can be defined as any probative information stored or transmitted in electronic form that may be legally presented at trial. As with any other type of evidence it is important for electronic evidence to have a direct bearing on the crime committed.
- Although the participants provided different meanings of the concept, the majority demonstrated a good understanding of the concept ‘electronic evidence’.
- The sample A participants had different views on where electronic evidence resort under the categories or types of evidence. The classification of electronic evidence by the participants varied between circumstantial evidence, documentary evidence and physical evidence. Two participants could not provide any response on where electronic evidence resorts under the categories or types of evidence.
- It has been found that South African courts find it difficult to classify electronic evidence. The courts deal with electronic evidence as either documentary or real evidence, and this depends on the evidence presented before them. There are instances where a computer printout may be dealt with as documentary evidence in

situations where a computer is operated by a person to generate such evidence. On the other hand a computer printout may be dealt with as real evidence because it was generated automatically without any interference from a human being.

- With regard to the difference between paper and electronic documents one of the expert participant pointed out that electronic evidence is not catered for in the existing rules of the law of evidence because these rules were designed specifically for paper documents hence the creation of the Electronic Communications and Transactions Act 25 of 2002 which is meant to address electronic evidence. This is an indication that there is a distinction between electronic and paper evidence although the information from a computer can be printed on paper and treated as a document, this does not mean that these types of evidence can be treated the same for the reason that they are physically different.
- It has also been found that another distinction between paper and electronic evidence is in the history of any electronic document which describes how, when and by whom an electronic document was created, modified and transmitted as it remains embedded in the computer system. A printed document may not show its history, for instance: the origins, contacts or edits carried out in the document Furthermore, if one shreds a paper document it will be completely destroyed and cannot be recovered
- It was further established that every piece of information captured electronically remains on a computer hard drive although it might appear deleted from the surface. Therefore, it is not easy to destroy electronic evidence.

6.2.1.3 Research question three: What are the standards or legal requirements for collecting and preserving electronic evidence?

- It was established from the expert participants that the Electronic Communication and Transactions Act 25 of 2002(a) does not provide guidelines for the collection of electronic evidence and in South Africa there are no procedures that have been tested by courts on the collection, preservation and analysis of electronic evidence.
- It has emerged from this research that there are established internationally recognised general standards and best practice procedures for the collection of electronic evidence and that these include but are not limited to identification, preservation, acquisition, authentication and analysis of electronic evidence. The

expert participants mentioned that law enforcement relies on the these international standards even though they have not been tailored into standard operating procedures aligned to the Electronic Communications and Transactions Act 25 of 2002.

- The sample A participants lacked knowledge on the established international standards designed specifically for collecting electronic evidence. 12 participants mentioned that the existing standard operating procedures on investigation and evidence collection in their department serve as guidance for investigators in collecting electronic evidence. Three participants suggested that these standards must be designed to deal specifically with electronic evidence since they deal with the collection of evidence in general. Six participants said that they rely on police officials to collect electronic evidence and four participants could not provide a response in this regard.

6.2.1.4 Research question four: Can information that has been interpreted through the use of a software tool be accepted as evidence at trial?

- Based on this research it has been found that the evidence presented through analysis software tools can only assist the court to visualize the evidence and provide an understanding of relationships and therefore cannot be used as a substitute for the actual evidence.
- A general finding in sample A participants is that the majority of the participants had never received any training on the use of analysis software tools and therefore do not have knowledge of the tools that can be used to interpret information. A lack of training on the use of analysis software tools is identified in this regard.

6.2.1.5 Research question five: Why is it important to maintain a chain of custody when collecting and preserving electronic evidence?

- It was established in this research that a chain of custody is considered necessary to protect the integrity of the evidence and to ensure that the evidence is trustworthy in that it has not been interfered with from the time of seizure to the time it was presented in court.
- Nine out of the 25 participants in sample A had a limited understanding of the importance of maintaining a chain of custody.

6.2.1.6 Research question six: What are the legal requirements for admissibility of electronic evidence at trial?

- It was established that the principles for the admissibility of evidence are relevance, reliability, and authenticity.
- The sample A participants could not provide appropriate answers on the legal requirements for admissibility of electronic evidence at trial which are relevance, reliability, and authenticity. However, five participants only said the evidence must be original.

6.2.2 Secondary findings

The researcher made certain secondary findings, based on the important issues that arose from the discussions under each chapter. These findings are outlined below.

6.2.2.1 The mandate to investigate crime

- It was found that not only the police have the mandate to investigate crime; various statutes also confer a certain degree of investigative power on corporate, private security and public sectors. However, even though these bodies are conferred with such powers, they still rely on the police if they wish to institute criminal proceedings against an accused.

6.2.2.2 Qualities of an investigator

- One important quality of a good investigator is to be independent in thinking, irrespective of any suspicions that the investigator might have. This requires the investigator not to rely on preconceived ideas but rather on facts to reach a fair conclusion.
- The sample A participants appeared to be knowledgeable and had a good understanding of the qualities required of a good investigator.

6.2.2.3 Objectives of investigation

- From the literature study, it was established that the objectives of investigation entail:
- Identification of a crime;
- Collection of evidence;
- Identification of the suspect;

- Securing of the attendance of the accused in court and
- Prosecution.
- The majority of sample A participants were familiar with the objectives of investigation.

6.2.2.4 The utilisation of experts

- The research revealed that experts are those people who are adequately trained to extract evidence from a computer system in such a way that they maintain a strict chain of custody, to ensure that the evidence is preserved in its original form and may be used in a court of law. They provide an interpretation of evidence in a court which is outside the experience and knowledge of the judiciary.
- The sample A participants appeared to be familiar with the reasons for using computer forensic experts. 18 participants reported that experts are more knowledgeable than ordinary employees because they are adequately trained to handle electronic evidence.
- It was also established from the expert participants in sample B that that not all investigators are skilled enough to handle electronic evidence and produce high quality evidence. A lack of specialist training aimed at crafting specialist skills in the field of investigation is identified in this regard.

6.2.2.5 Presentation of electronic evidence in court

- The sample A participants demonstrated a good understanding of how evidence should be presented in court. They mentioned that the investigator should be well prepared about the case to be presented; furthermore the presentation should be made in a way that makes it possible to understand the evidence presented and that the investigator should provide all pertinent information on the case. It was revealed by the expert participants that the investigator must provide a detailed explanation on the procedures followed when evidence was seized and demonstrate that there was continuity on the handling of the evidence from the time it was seized to the time it was analysed at another location.

6.2.2.6 Challenges of electronic evidence in prosecution

- It has been established through this research that investigators have not been adequately trained and do not have the high level of technical expertise needed to deal with electronic evidence.

- It was also established from the expert participants in sample B that an average judiciary does not have a good enough understanding of technology to enable it to rule effectively on electronic evidence; as a result some cases are thrown out of court.
- Eight participants in sample A did not have any understanding of the real challenges faced by prosecution when dealing with electronic evidence as they responded by saying that electronic evidence is too complicated to understand. The 17 remaining participants appeared to have an understanding of the problems encountered in dealing with electronic evidence.

6.3 Recommendations

The recommendations in this study are based on the findings of the study and the body of literature reviewed.

6.3.1 Standards for collecting electronic evidence

- It is recommended that standards specific to the collection of electronic evidence be developed for South Africa to guide law enforcement in dealing with and ensuring the admissibility of such evidence at trial.

6.3.2 Training

- The collection, preservation, analysis and presentation of electronic evidence require a high level of expertise because technology is continuing to develop and is becoming increasingly complex. Training is needed to address the lack of knowledge and expertise amongst investigators in handling electronic evidence and ensuring the admissibility of such evidence at trial.
- It is recommended that guidelines be compiled and training programmes be developed for all investigators. The programmes should be aimed at continuous development for law enforcement officers on the collection, analysis and presentation of electronic evidence. The training should also help investigators to acquire a basic working knowledge of the technical aspects of electronic evidence in general. Both the judiciary and investigators should master the specific technical details of cases dealing with electronic evidence.

- It is also recommended that investigators be trained on the use of analysis software tools.

6.3.3 Additional research

- It is recommended that once standards for the collection, preservation, analysis and presentation of electronic evidence are developed and used by law enforcement, additional research be conducted to monitor and evaluate the effectiveness of these standards.

6.4 Summary

The primary findings of this research have addressed the research questions and shown that there are existing general forensic standards that can be followed by law enforcement in the collection, analysis and presentation of electronic evidence. The integrity and authenticity of electronic evidence collected should be ensured at all times. By following the methodologies correctly, law enforcement can ensure the admissibility of the evidence in court.

The secondary findings have revealed that law enforcement encounters problems in dealing with electronic evidence. This is because proper procedures are not followed in the collection, analysis and presentation of electronic evidence. Law enforcement is not adequately skilled and there are no training programmes in place to ensure continuous development of officials. The lack of set standards in place to guide law enforcement in the collection, handling and presentation of electronic evidence also adds to the problem. Standard operating procedures as well as training should provide investigators with a clear knowledge of adequate electronic evidence handling practices.

A number of recommendations have been made, based on the findings of the research. The recommendations are aimed at improving the methods of collection, analysis and presentation of electronic evidence at trial. Computer crime is here to stay and the time has come for all role players to acknowledge the importance of the use of electronic evidence in investigation. Further research on computer evidence is strongly recommended to keep abreast with new developments in cyber crime investigations.

LIST OF REFERENCES

American Heritage Dictionary of the English Language. 2003. s.v. "investigator". Boston: Houghton.

Anson, S. & Bunting, S. 2007. *Mastering windows network forensics and investigation* Indianapolis: Wiley Publishing.

Auditing Profession Act see South Africa. 2005.

Bailey, W.G. 1995. *The encyclopedia of police science*. 2nd edition. New York: Garland.

Balkin, J.M., Grimmelmmann, J., Katz, E., Kozolvski, N. & Zarsky, T. 2007. *Cybercrime: Digital cops in a networked environment.* New York: New York University Press.

Banks, F.Z. 2002. *Corporate legal compliance handbook.* New York: Aspen Publishers.

Bantekas, I. & Nash, S. 2003. *International criminal law*. 2nd edition. London: Routledge-Cavendish.

Barbara, J.J. 2008. *Handbook of digital and multimedia forensic evidence*. New Jersey: Humana Press.

Bergman, P. & Berman-Barrett, S.J. 2008. *The criminal law handbook: Know your rights, survive the system.* Berkeley: Nolo.

Best practices for seizing electronic evidence: A pocket guide for first responder. 2006. United States Secret Service. From: http://www.forwardedge2.com/pdf/ bestpractices.pdf (accessed 14 December 2009).

Bester, B. 2002. Crime scene management. *Servamus*, 92(1), January:28-29.

Broadhurst, R.G. & Grabosky, P.N. 2005. *Cyber-crime: The challenge in Asia.* Hong Kong: Hong Kong University Press.

Bryant, R. 2008. *Investigating digital crime.* London: John Wiley & Sons Ltd.

Byrd, M. 2004. *Duty description to the crime scene investigator*. Miami: Miami Dade Police Department.

Callanan, T. 1992. *Principles of crime investigation: Training manual for investigation.* Pretoria: SAPS.

Caloyannides, M.A. 2004. *Privacy protection and computer forensics.* 2nd edition. Norwood: Artech House.

Cardwell, K., Clinton, T., Cohen, T., Collins, E., Cornell, J., Cross, M., Depew, L., Ehuan, A., Gregg, M., Jean, B.R., O'Shea, K., Reis, K., Reyes, A., Schuler, K., Schneider, S., Schroader, A., Varsalone, J., Wiles, J. & Wright, C. 2007. *The best damn cybercrime and*

digital forensics book period. Burlington: Syngress Publishing.

Carmichael, D.R., Whittington, R. & Graham, L. 2007. *Accountants' handbook.* 11th edition. New York: John Wiley & Sons.

Casey, E. 2000. *Digital evidence and computer crime: Forensic science, computers, and the internet.* Florida: Academic Press.

Casey, E. 2002. Practical approaches to recovering encrypted digital evidence. *International Journal of Digital Evidence,* 3(1)

Casey, E. 2004. *Digital evidence and computer crime: Forensic Science, computers and the internet.* 2nd edition. Florida: Academic Press.

Chisum, W.J. & Turvey, B. 2000. Evidence dynamic: Locard's exchange principle. Crime Reconstruction. *Journal of Behavioral Profiling*, 1, January:1-15.

Christopher, B.L.T. 2007. *Computer evidence: Collection and preservation.* Rockland, MA:Charles River Media.

Civil Proceedings Evidence Act see South Africa. 1965.

Computer Evidence Act see South Africa. 1983.

Constitution of the Republic of South Africa see South Africa. 1996 (a).

Craiger, J.P., Pollitt, M. & Swauger, J. 2005. *Law enforcement and digital evidence.* New York: John Wiley & Sons.

Craiger, J. P., Swauger, J. & Marberry, C. 2005. *Digital evidence obfuscation: recovery techniques*. National Center for Forensic Science: University of Central Florida. Orlando. From: http//www.ncfs.org/craiger.5778-85. SPIE .pdf (accessed 20 September 2010)

Craiger, J.P. & Shenoi, S. 2007. *Advances in digital forensics III.* Boston: Springer.

Crayton, C.A. 2003. *Security exam guide.* Florida: Cengage Learning.

Creswell, J.W. 1994. *Research design, qualitative and quantitative approaches.* New Delhi: SAGE.

Criminal Procedure Act see South Africa. 1977.

Cross, M. 2008. *Scene of the cybercrime.* 2nd edition. Arlington: Syngress Publishing.

Denscombe, M. 2002. *Ground rules for good research: A 10 point guide for social researchers.* Philadelphia: Open University Press.

Denscombe, M. 2003. *The good research guide.* Philadelphia: Open University Press.

De Vos, A.S. 1998. *Research at grass roots: A primer for the caring professions.* Pretoria: Van Schaik.

De Vos, A.S., Strydom, H., Fouche, C.B. & Delport, C.S.L. 2005. *Research at grass roots: For the social sciences and human service profession.* 3rd edition. Van Schaik.

Dowling, J.L. 1997. *Criminal investigation.* Texas: Sam Houston State University.

Duerr, T.E., Beser, N.D. & Staisiunas, G.P. 2004. Information Assurance Applied to authentication of Digital Evidence. *Forensic Science Communications,* 6(4) October:1.

Electronic Communication and Transactions Act see South Africa. 2002(a).

Feigenson, N. & Dunn, M. 2003. New visual technologies in court: Directions for research. *LAW & HUM. BEHAV,* 27:109-110. From: www.springerlink.com/indexM0M8334 31X226870.pdf (accessed 16 February 2009).

Fisher, B.A.J. 2004. *Techniques of crime scene investigation.* 7th edition. Washington D.C: CRC.

Fisher, B.A.J. & Fisher, D. 2003. *Techniques of crime scene investigation.* 7th edition. New York: CRC Press.

Flick, U. 2002. *An introduction to qualitative research.* 2nd edition. London: SAGE.

Francoeur, J. 2003. *White Paper: The principles of electronic agreement legal admissibility. Ada: Proof Space*. From:http://www.scribd.com/doc/276157/ The-Principles-of- Electronic-Agreement-Legal- Admissibility-WP-8-07 (accessed 5 April 2008).

Gahtan, A.M. 1999. *Electronic evidence.* Canada: Carswell Thomson Publishing.

Gallagher, S.R & Aro, E.P. 2005. *Evolving standards for discovery in the electronic age.* Colorado: Hogan & Hartson. From:http://www.abanet.org/buslaw/newsletter/0036/ materials/pp8.pdf (accessed 15 December 2009).

Galves, F. 2000. Where the not-so-wild things are: Computers in the courtroom, the federal rules of evidence, and the need for institutional reform and more judicial acceptance .*Harvard Journal of Law & Technology,* 161(13): 229-230.

Galves, F. & Galves, C. 2004. Ensuring the admissibility of electronic forensic evidence and enhancing its probative value at trial. *Criminal Justice Magazine,* 19(1):3. From: http ://www.abanet.org/crimjust/cjmag/home.html (accessed 25 September 2008).

Gardner, R.M. 2005. *Practical crime scene processing and investigation*. Washington D.C.: CRC.

Genge, N.E. 2002. *The forensic casebook.* New York: Ballantine Books.

Golden, T.W., Skalak, S.L. & Clayton, M.M. 2006. *A guide to forensic accounting investigation.* New Jersey: John Wiley & Sons.

Greene, J.R. 2006. *The encyclopedia of police science.* 3rd edition. Florida: CRC Press.

Hatch, B. 2008. *Hacking exposed linux.* 3rd edition. Emeryville, CA: McGraw Hill Osborne Media.

Hedley, S. 2006. *The law of electronic commerce and the internet in the UK and Ireland*. London: Routledge-Cavendish.

Hofman, J. 2006. *Electronic evidence in South Africa*. From: http://hofman@law.uct.ac.za (accessed on 21 February 2009).

Holland, J. & Campbell, J. 2005. *Methods in development research.* London: ITDG.

Holmes, S. 2006. *An overview of criminal investigation.* New York: Clarkson N. Potter. From: http://www.apsu.edu/oconnort/3220/3220lect01.htm (accessed 7 December 2008).

Horswell, J. 2004. *The practice of crime scene investigation.* Washington D.C.: CRC.

Hrycko, O. 2007. *Electronic discovery in Canada: Best practices and guidelines*. Toronto: CCH Canadian.

Immigration Act see South Africa. 2002(b).

Jacko, J.A., Stephanidis, C. & Harris, D. 2003. *Human-computer interaction: Theory and practice.* London: Lawrence Erlbaum Associates.

Johnson, E.S. 1981. *Research methods in criminology and criminal justice.* New Jersey: Prentice Hall.

Joubert, C. 2001. *Applied law for police officials.* 2nd edition. Cape Town: Juta Legal and Academic Publishers.

Kanellis, P. 2006. *Digital crime and forensic science in cyberspace.* London: Idea Group Inc.

Karagiozis, M.F. & Sgaglio, R. 2005. *Forensic investigation handbook: An introduction to the collection, preservation, analysis and presentation of evidence*. Illionis: Charles C Thomas Publisher.

Kaufmann-Kohler, G. & Schultz, T. 2004. *Online dispute resolution: Challenges for contemporary justice.* Netherlands: Kluwer Law International.

Keane, A. 2000. *The modern law of evidence.* 5th edition. London: Butterworths.

Keena, J.R. 2002. *E-Discovery: Unearthing documents byte by byte.* Minnesota. From: http://www.mnbar.org/benchandbar/2002/mar02/ediscovery.htm (accessed 5 April 2008).

Kenneally, E.E. 2005. *Confluence of digital evidence and the law: On the forensic soundness of live-remote digital evidence collection*. Los Angeles: University of California.

Kennedy, R.B. 2004. *International association for identification*. London. From: http://www.theiai.org. (accessed 12 March 2008).

Kipper, G. 2007. *Wireless crime and forensic investigation.* New York: Taylor & Francis Group.

Kleiman, D. 2007. *Official CHFI (exam 312-49) study guide for computer hacking forensics investigators*. Massachusetts: Syngress.

Kovacich, G.L. & Boni, W.C. 2000. *High-technology-crime investigator's handbook: Working in the global information environment*. Burlington: Butterworth-Heinemann Publications.

Kovacich, G.L. & Jones, A. 2006. *High-technology crime investigator's handbook: Establishing and managing a high-technology crime prevention program*. 2nd edition. Washington: Butterworth-Heinemann Publications.

Kozushko, H. 2003. *Digital evidence graduate seminar*. New Mexico Tech-Computer Science Department. From: http://www.infosyssec.org/infosyssec/.../forensic evidence1.html (accessed 3 March 2009).

Lambrechts, D. 2001. Forensic investigation. Pollex. *Servamus*, 94(10):93.

Lange, M.C.S. & Nimsger, K.M. 2004. *Electronic evidence and discovery: What every lawyer should know.* Chicago: ABA Publishing.

Lange, M.C.S. & Nimsger, K.M. 2009. 2nd edition. *Electronic evidence and discovery: What every lawyer should know.* Chicago: ABA Publishing.

Laryea, E.T. 2002. *Paperless trade: Opportunities, challenges and solutions*. London: Kluwer Law International.

Laryea, E.T. 2003. *Paperless trade: Opportunities, challenges and solutions.* Netherlands: Kluwer Law International.

Law of Evidence Amendment Act see South Africa. 1988(a).

Lee, H.C. & Harris, H.A. 2000. *Physical evidence in forensic science.* Tucson: Lawyers & Judges.

Lee, H.C., Palmbach,T. & Miller, M.T. 2003. *Crime scene handbook.* London: Academic.

Leedy, P.D. 1997. *Practical research planning and design.* New Jersey: Prentice Hall.

Leedy, P.D. & Ormrod, J.E. 2001. *Practical research: Planning and design.* 7th edition. Upper Saddle River: Merrill Prentice Hall.

Leedy, P.D. & Ormrod, J.E. 2005. *Practical research: Planning and design.* 8th edition. Ohio: Merrill Prentice Hall.

Lentini, J.J. & Lentini, J.L. 2006. *Scientific protocols for fire investigation.* Florida: CRC Press.

LexisNexis. 2007. *Embedded information in electronic document*. From: http://www .lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADIMetaData.pdf. (accessed 25 September 2008).

MacNeil, H. 2000. *Trusting records: Legal, historical and diplomatic perspectives*. New York: Springer.

Marais, C.W. & Van Rooyen, J.N. 1994. *Crime investigation.* 4th edition. Pretoria: Promedia.

Marcella, A.J. & Greenfield, R.S. 2002. *Cyber forensics: A field manual for collecting, examining and preserving evidence of computer crimes*. London: Taylor & Francis.

Marcella, A.J., Marcella-Jr, A.J. & Menendez, D. 2007. *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes*. 2nd edition. Florida: CRC Press.

Marud, M. 2004. *Argus*, 27 May: 28

Mason, S. 2006. *Authentication of electronic evidence.* Information Age. From: http://www infoage.idg.com.au/index.php/id;1288698068;fp;4;fpid;675408222 (accessed 2 February 2009).

Maxfield, M.G. & Babbie, E. 1995. *Research methods for criminal justice and criminology*. Boston: Thomson-Wadsworth.

McMillan, J. H. & Schumacher, S. 2001. *Research in education: A conceptual introduction* 5th edition. New York: Longman.

Miles, M.B. & Huberman, A.M. 1994. *Qualitative data analysis.* 2nd edition. London: SAGE Publications.

Mohay, G.M., Anderson, A., Collie, B., De Vel., O. & McKemmish, R.D. 2003. *Computer and intrusion forensics.* Boston: Artech House.

Mouton, J. 1996. *Understanding social research.* Pretoria: Van Schaik.

Mouton, J. 2001. *How to succeed in your master's and doctoral studies.* Pretoria: Van Schaik.

Mozayani, A. & Noziglia, C. 2006. *The forensic laboratory handbook: Procedures and practice.* New Jersey: Humana Press.

Nelson, S.D., Olson, B.A. & Simek, J.W. 2006. *The electronic evidence and discovery handbook: Forms, checklists, and guidelines.* Chicago: American Bar Association.

Neuman, W.L. 1997. *Social research methods: Qualitative and quantitative approaches.* 3rd edition. Needham Heights, MA: Allyn & Bacon.

Neumeier, M.M., Hansen, B.D. & Dmitrieva, I.Y. 2003. *Paper or plastic? – The hunt for electronic treasure during discovery.* Chicago: Jenner & Block.

Ogle, R.R. 2004. *Crime scene investigation and reconstruction.* New Jersey: Pearson Education.

O'Hara, C. 1962. *Modern criminal investigation*. 5th edition. New York: Funk & Wagnalls.

Overly, M.R. 1999. *Cybercrime and the rules on electronic evidence: Overly on electronic evidence in California*. San Francisco: West Group.

Oxford Advanced Learners Dictionary. 1989. New edition. s.v. "admissibility". Oxford: Oxford University Press.

Palm, Y. 2000. *Basic aspects of document related investigations*. Pretoria: Government Printer.

Palmiotto, M.J. 1998. *Criminal investigations.* 2nd edition. Wichita: Austin & Winfield.

Parlade, C.V. 2004. *Cyberspace police center for Asia pacific*. Phillipines. From: http://www.ecapproject.org/fileadmin/ecapII/pdf/en/activities/national/Philippines/2004102526/attyparladecybercrime.pdf (accessed 23 May 2008).

Participant 1, Investigator at Department of Home Affairs. Statement to author, 15 April 2009. Pretoria.

Participant 2, Investigator at Department of Home Affairs. Statement to author, 15 April 2009. Pretoria.

Participant 3, Investigator at Department of Home Affairs. Statement to author, 15 April 2009. Pretoria.

Participant 4, Investigator at Department of Home Affairs. Statement to author, 15 April 2009. Pretoria.

Participant 5, Investigator at Department of Home Affairs. Statement to author, 16 April 2009. Pretoria.

Participant 6, Investigator at Department of Home Affairs. Statement to author, 16 April 2009. Pretoria.

Participant 7, Investigator at Department of Home Affairs. Statement to author, 16 April 2009. Pretoria.

Participant 8, Investigator at Department of Home Affairs. Statement to author, 16 April 2009. Pretoria.

Participant 9, Investigator at Department of Home Affairs. Statement to author, 11 May 2009. Pretoria.

Participant 10, Investigator at Department of Home Affairs. Statement to author, 11 May 2009. Pretoria.

Participant 11, Investigator at Department of Home Affairs. Statement to author, 11 May 2009. Pretoria.

Participant 12, Investigator at Department of Home Affairs. Statement to author, 11 May 2009. Pretoria.

Participant 13, Investigator at Department of Home Affairs. Statement to author,12 May 2009. Pretoria.

Participant 14, Investigator at Department of Home Affairs. Statement to author, 12 May 2009. Pretoria.

Participant 15, Investigator at Department of Home Affairs. Statement to author, 12 May 2009. Pretoria.

Participant 16, Investigator at Department of Home Affairs. Statement to author, 12 May 2009. Pretoria.

Participant 17, Investigator at Department of Home Affairs. Statement to author, 12 May 2009. Pretoria.

Participant 18, Investigator at Department of Home Affairs. Statement to author, 14 May 2009. Pretoria.

Participant 19, Investigator at Department of Home Affairs. Statement to author, 14 May 2009. Pretoria.

Participant 20, Investigator at Department of Home Affairs. Statement to author, 14 May 2009. Pretoria.

Participant 21, Investigator at Department of Home Affairs. Statement to author, 14 May 2009. Pretoria.

Participant 22, Investigator at Department of Home Affairs. Statement to author, 15 May 2009. Pretoria.

Participant 23, Investigator at Department of Home Affairs. Statement to author, 15 May 2009. Pretoria.

Participant 24, Investigator at Department of Home Affairs. Statement to author, 15 May 2009. Pretoria.

Participant 25, Investigator at Department of Home Affairs. Statement to author, 15 May 2009. Pretoria.

Participant 26, Computer Forensic Specialist at South African Police Service. Statement to author, 1 October 2009. Pretoria.

Participant 27, Computer Forensic Specialist at Telkom. Statement to author, 2 October 2009. Pretoria.

Participant 28, Doctor in Cyber Forensics at A2 Consulting-Computer Forensics. Statement to author, 25 October 2009. Pretoria.

Participant 29, Professor at University of South Africa. Statement to author, 25 September 2009. Pretoria.

Participant 30, Professor at University of Cape Town. Statement to author, 27 October 2009. Cape Town.

Pearlstein, D.J. 2002. *Antitrust law development.* 5th edition. California: American Bar Association.

Philipp, A., Cowen, D. & Davis, C. 2009. *Hacking exposed computer forensics.* 2nd edition. New York: McGraw-Hill.

Pollitt, M.M. 2001. Report on digital evidence: Paper delivered at the 13th International Criminal Police Organization forensic science symposium. From: http://www.interpol.int/public/Forensic/IFSS/meeting13/Reviews/Digital.pdf (accessed 3 February 2009).

Prevention and Combating of Corrupt Activities Act see South Africa. 2004.

Private Security Industry Regulation Act see South Africa. 2001.

Public Record Office Victoria (PROV). 2003. Electronic records as evidence. From: http://www.prov.vic.gov.au/publications/publns/PROVRMadvice8.pdf (accessed 23 May 2009).

Raysman, R. & Brown, P. 1984. *Computer law: Drafting and negotiating forms and agreements*. New York: Law Journal Press.

Reference Method for UNISA. 2004. 3rd edition. Florida: UNISA.

Regulation of Interception of Communications and Provision of Communication- related Information Act see South Africa. 2002(c).

Ritter, N. 2006. Digital Evidence: How law enforcement can level the playing field with criminals, *NIJ Journal,* (254):21. From: http://www.ncjrs.gov/pdffiles1/jr000254.pdf (accessed 12 May 2009).

Robbins, M.D. 1999. Computers and the discovery of evidence – A new dimension to civil procedure. *17 John Marshall J of Comp. & Info. Law*, (2): 411.From: http://www.jcil.org/journal/articles/204.html (accessed 18 June 2008).

Sarantakos, S. 1998. *Social research*. 2nd edition. London: Macmillan.

Schetina, E.S., Green, K. & Carlson, J. 2002. *Internet site security.* Boston, MA: Addison-Wesley.

Schmidt, C.W.H. & Rademeyer, H. 2006. *Law of evidence*. Durban: Butterworths.

Schwikkard, P.J. & Van der Merwe, S.E. 2009. *Principles of evidence.* 3rd edition. Cape Town: Juta.

Sennewald, C. A. & Tsukayama, J.K. 2006. *Process of investigation: Concepts and strategies for investigators in the private sector.* 3rd edition. Woburn: Elsevier Butterworth-Heinemann.

Shah, G. 2002. *Investigation of crime and criminals.* New Delhi: Anmol Publications.

Shira, A., Scheindlin, S.A. & Rabkin, J. 2000. Electronic discovery in federal civil litigation: Is rule 34 up to the task? *B. C. L. Rev*, 41(2) March:327-338.From: http://www.bc.edu/bc_org/avp/law/lwsch/journals/bclawr/412/03FMS.html (accessed 23 May 2008).

Silvernail, S.J. 1997. Electronic Evidence: Discovery in the Computer Age. *The Alabama Lawyer,* 58, May:176-177.

Simms, B.W. & Petersen, E.R. 1991. An information processing model of a police organization. *Management Science*, 37(2), February:216.

Smith, R.G., Grabosky, P.N. & Urbas, G. 2004. *Cyber criminals on trial.* Melbourne: Cambridge University Press.

South Africa. 1965. *Civil Proceedings Evidence Act 25 of 1965*. Pretoria: Government Printer.

South Africa. 1977. *Criminal Procedure Act 51 of 1977.* Pretoria: Government Printer.

South Africa. 1983. *Computer Evidence Act 57 of 1983.* Pretoria: Government Printer.

South Africa. 1988(a). *Law of Evidence Amendment Act 45 of 1988*. Pretoria: Government Printer.

South Africa. 1988(b). *South African Police Service Act 68 of 1988.* Pretoria: Government Printer.

South Africa. 1993. *South African Interim Constitution Act 200 of 1993*. Pretoria: Government Printer.

South Africa. 1996(a). *Constitution of the Republic of South Africa 108 of 1996.* Pretoria: Government Printer.

South Africa. 1996(b). *Special Investigating Unit and Special Tribunal Act 74 of 1996.* Pretoria: Government Printer.

South Africa. 2001. *Private Security Industry Regulation Act 56 of 2001*. Pretoria: Government Printer.

South Africa. 2002(a). *Electronic Communication and Transactions Act 25 of 2002.* Pretoria: Government Printer.

South Africa. 2002(b). *Immigration Act 13 of 2002.* Pretoria: Government Printer.

South Africa. 2002(c). *Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.* Pretoria: Government Printer.

South Africa. 2004. *Prevention and Combating of Corrupt Activities Act 12 of 2004.* Pretoria: Government Printer.

South African Interim Constitution Act see South Africa. 1993.

South African Police Service Act see South Africa. 1988(b).

South African Law Commission. 1995. Project 95: *Investigation into the Computer Evidence Act 57 of 1983, Working Paper 60*. Pretoria: The Commission.

Special Investigating Unit and Special Tribunal Act see South Africa. 1996.

Stephenson, P. 2000. *Investigating computer-related crime.* Florida: CRC Press.

Sterneckert, A.B. 2003. *Critical incident management.* Florida: CRC Press.

Stippich, M.J. 2006. *Electronic evidence: Issues.* Wisconsin: Wisconsin Bar Association. From:https://www.wisbar.org/AM/TemplateRedirect.cfm?template=/CM/ContentDisplay.cfm&ContentID=61964 (accessed 2 May 2009).

Stockdale, J.E. & Gresham, P.J. 1995. *The presentation of police evidence in court: police research group police research series: Paper number 15*. Home Office Police Research Group (PRG). From: http://www.homeoffice.gov.uk/rds/prgpdfs/fprs15.pdf (accessed 2 June 2008).

Swanepoel, J. 2001. *Rights and powers of private investigation*: Paper delivered at the second world conference on modern criminal investigation, organised crime and human rights. Durban. 3-7 December 2001.

Swanson, C.R., Chamelin, N.C. & Territo, L. 2003. *Criminal investigation*. 8th edition. Boston: McCraw-Hill.

Taylor, R.B. 1994. *Research methods in criminal justice.* Sydney: McGraw-Hill.

Taylor, C. 2003. *An introduction to metadata.* University of Queensland Library. From:

http://74.125.77.132/search?q=cache:1koOCagFsgJ:www.library.uq.edu.au/iad/ctmmeta4.html+metadata&cd=2&hl=en&ct=clnk (accessed 3 May 2008).

Technical Working Group for Electronic Crime Scene Investigation. 2001. *Electronic Crime scene investigation: A guide for first responders.* National Institute of Justice. From: http://www.ncjrs.gov/pdffiles1/nij/187736.pdf (accessed 8 November 2008).

The strategic value of electronic discovery. 2007. Infology. From: http://www.infology.net/downloads/The%20Strategic%20Value%20of%20Electronic%20Discovery.pdf. (accessed 12 June 2009).

Thornhill, T.W. 1995. *Forensic accounting: How to investigate financial fraud*. New York: Irwin.

Thornton, L., Carrim, Y., Mtshaulana, P. & Reburn, P. 2006. *Telecommunications law.* Johannesburg: STE Publishers.

Tipton, H.F. & Krause, M. 2003. *Information security management handbook.* 4th edition. Florida: CRC Press.

Tipton, H.F. & Krause, M. 2006. *Information security management handbook.* 5th edition. Florida: CRC Press.

Vacca, J. 2005. *Computer forensics – Computer crime scene investigation.* 2nd edition. Hingham: Charles River Media.

Vadackumchery, J. 2003. *Crime law and police science.* New Delhi: Concept Publishing Company.

Van der Merwe, C.G. & Du Plessis, J.E. 2004. *Introduction to the law of South Africa.* Netherlands: Aspen Publishers.

Van der Merwe, D., Roos, A., Pistorius, T. & Eiselen, S. 2008. *Information and communications technology law.* Durban: LexisNexis.

Van der Westhuizen, J. 1996. *Forensic criminalistic.* 2nd edition. Johannesburg: Heinemann.

Van Rooyen, H.J.N. 2004. *The A-Z of investigation: A practical guide for private and corporate investigators.* Pretoria: Crime Solve.

Velasco, J.A. 2007. *A guide to electronic evidence collection methodologies*. New York: Merrill Legal Solutions. From: http://www.renewdata.com/promos/EE-Collection-Methodologies-Whitepaper.pdf (accessed 05 June 2008).

Vere, A. 2009. Legal and regulatory frameworks for the knowledge economy: Concept

paper for first session of the Committee on Development Information, Science and Technology (CODIST-I). United Nations Economic Commission for Africa (UNECA). From: http://www.uneca.org/codist/codist1/content/E-ECA-CODIST-1-15-EN.pdf (accessed on 18 February 2010).

Volonino, L. 2003. Electronic evidence and computer forensics. *Communications of the Association for Information Systems,* 12(27):October:7. From: http://138.92.8.227/Volonino-CAIS-Journal.pdf. (accessed 20 May 2009).

Wang, S.J. 2007. Measures of retaining digital evidence to prosecute computer based cyber crimes. *Computer Standards & Interfaces, 29*(2):8.

Ward, R.H. 1975. *Introduction to criminal investigation.* Philippines: Addison-Wesley Publishing Company.

Welman, J.C. & Kruger, S.J. 1999. *Research methodology for the business and administrative sciences.* Halfway house: International Thompson Publishing.

Welman, J.C. & Kruger, S.J. 2001. *Research methodology for the business and administrative science.* Cape Town: Oxford University Press.

Welman, J.C. & Kruger, S.J. 2002. *Research methodology*. 2nd edition. Cape Town: Oxford University Press.

Weston, P.B., Lushbaugh, C. & Wells, K.M. 2000. *Criminal investigation: Basic perspectives*. New Jersey: Prentice Hall.

Williams, R. 2000. *Explaining corruption.* Cheltenham: Edgar Publishing.

Winn, J.K. & Wright, B. 2000. *The law of electronic commerce*. 3rd edition. New York: Aspen Publishers.

Zeffert, D.T., Paizes, A.P. & St Q Skeen, A. 2003. *The South African law of evidence.* Durban: Butterworths.

Zondo-Kabini, H. 2003. Application of the Electronic Communications and Transactions Act to online merchants from other jurisdictions. *Northwestern Journal of Technology and Intellectual Property,* 1(1):78. From: http://www.law.Northwestern.Edu/journals/njtip/v1/n1/7NJTIP (accessed 15 April 2009).

Zysman, A. 2006. *Forensic accounting demystified.* Zysman Forensic Accounting. From: http://www.forensicaccounting.com/one.htm#start (accessed 13 October 2007).

LIST OF CASES

Barclays Western Bank Ltd v Creser (2) SA 104 (T) 106

Estate De Wet v De Wet 1924 CPD 341

Ex Parte Rosch 1998 1 AII SA 319 (W)

Goliath v Fedgen Insurance 1994 2 PHF 31 (E)

Key v Attorney-General, Cape Provincial Division (1996) (6) BCLR 788 (CC)

Mabona v Minister of Law and Order 1988 (2) SA 654 SE at 660 D

Mdani v Allianz Insurance Ltd 1991 (1) SA 184 (A)

Minister of Safety and Security v Bennett [2007] SCA 139 (RSA)

Minister of Safety and Security v Liddell (247/2001) [2002] ZAECHC 5

Moloko v Ntsoane and Others 2004 (JR 1568/02) ZALC 35

S v Botha and Others (1) 1995 (2) SARC 598 (w)

S v De Villiers (1993) (1) SACR 574 (Nm)

S v Harper 1981 1 SA 88 D

S v Ndiki and Others 2008 (2) SACR 252 (Ck)

R v Schaube-Kuffer 1969 2 SA 40 (RA)

ANNEXURE A

Interview Schedule for Investigators

The use of electronic evidence in forensic investigation

Research questions

- What is forensic investigation?
- What is electronic evidence?
- How can electronic evidence be collected without compromising its integrity or credibility at trial?
- What are the legal requirements for admissibility of electronic evidence?

Historical Information

- How many years have you been an investigator?
- What type of investigations do you specialize in?
- Do you work for the private or public sector?
- What are your tertiary qualifications?
- Did you receive any formal training in computer crimes investigations?
- How old are you?

FORENSIC INVESTIGATION

1. What do you understand under the concept "forensic investigations?"
2. Who has the mandate to conduct investigations?
3. What qualities should an investigator have?
4. What are the responsibilities of an investigator?
5. What are the objectives of a forensic investigation?

ELECTRONIC EVIDENCE

6. What do you understand under the concept “electronic evidence”?
7. What are the types of evidence?
8. Where does electronic evidence resort under the categories or types of evidence?
9. What is the difference between electronic evidence and paper evidence?

COLLECTION OF ELECTRONIC EVIDENCE

10. What are the standards or legal requirements for collecting and preserving electronic evidence?
11. Can information that has been interpreted through the use of a software tool be accepted as evidence at trial?
12. Why is it important to maintain a chain of custody when collecting and preserving electronic evidence?
13. Why should computer forensic experts be used in the collection of electronic evidence?

LEGAL REQUIREMENTS FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE

14. Which legislation can be relied on for admissibility of electronic evidence?
15. What are the legal requirements for admissibility of electronic evidence?
16. How should evidence be presented in court?
17. What are the challenges faced by prosecution in dealing with electronic evidence?

ANNEXURE B

Interview Schedule for Expert Participants

The use of electronic evidence in forensic investigation

Research questions

- what is forensic investigation?
- What is electronic evidence?
- How can electronic evidence be collected without compromising its integrity or credibility at trial?
- What are the legal requirements for admissibility of electronic evidence?

ELECTRONIC EVIDENCE

1. Where does electronic evidence resort under the categories or types of evidence?
2. What is the difference between electronic evidence and paper evidence?

COLLECTION OF ELECTRONIC EVIDENCE

3. What are the standards or legal requirements for collecting and preserving electronic evidence?
4. Can information that has been interpreted through the use of a software tool be accepted as evidence at trial?
5. What information should be documented as proof that a chain of custody was maintained in handling evidence?
6. Why is it important to maintain a chain of custody when collecting and preserving electronic evidence?
7. Why should computer forensic experts be used in the collection of electronic evidence?

LEGAL REQUIREMENTS FOR ADMISSIBILITY OF ELECTRONIC EVIDENCE

8. Which legislation can be relied on for admissibility of electronic evidence?
9. What are the legal requirements for admissibility of electronic evidence?"

10. How should evidence be presented in court?
11. What are the challenges faced by prosecution in dealing with electronic evidence?