The impact of electronic evidence in forensic accounting investigations

W Janse van Rensburg

20546556

Dissertation submitted in full fulfillment of the requirements for the degree *Magister Commercii* in Forensic Accounting at the Potchefstroom Campus of the North-West University

Supervisor: Mr D Aslett

May 2014

Acknowledgements

I am deeply grateful for all the love and support I have received during the completion of this dissertation.

I would like to express special thanks to the following people:

- My father, Paul Janse van Rensburg;
- My mother, Ebeth Janse van Rensburg, who passed away on 23 April 2013 and even on her deathbed, was supportive of everything I did;
- My brother and sister, Paul and Hanri Janse van Rensburg;
- My supervisor, Duane Aslett, for all his assistance and input;
- Isabel Swart, from the Language Directorate of the North-West University, Potchefstroom Campus.
- My friends and family; and
- My colleagues at KPMG.

"Selfs al gaan ek deur donker dieptes, sal ek nie bang wees nie, want U is by my. In U hande is ek veilig." – Psalm 23:4

Abstract

This study revolves around the admissibility of electronic evidence obtained during forensic accounting investigations. Electronic evidence is problematic for the forensic accountant, in that the courts have difficulties with the admissibility of electronic evidence. The research method used in this dissertation is a literature study or literature review.

Firstly, the study aims to define a forensic accountant. The need for the forensic accountant is determined, as well as the definition and the roles and responsibilities of the forensic accountant. The study further aims to establish how the forensic accountant is regulated in South Africa.

Secondly, this study aims to provide a historical overview of South African legislation that addresses electronic evidence. Applicable legislation is the *Electronic Communications and Transactions Act 25 of 2002*, the *Criminal Procedure Act 51 of 1977*, the *Law of Evidence Amendment Act 45 of 1988*, the *Civil Proceedings Evidence Act 25 of 1965* and the repealed *Computer Evidence Act 57 of 1983*.

To determine the challenges that arise from electronic evidence, it is critical to understand how electronic evidence is classified in terms of the traditional forms of evidence. Documentary evidence, real evidence and evidence as the product of an apparatus, with specific reference to electronic evidence, is discussed for the purpose of this study.

Hearsay evidence, the originality of electronic evidence, as well as the authenticity and reliability of electronic evidence hamper the admissibility of electronic evidence. The impact of legislation on the aforementioned difficulties is considered in this study.

The problematic nature of electronic evidence already creates challenges during legal proceedings. The forensic accountant can follow certain steps and procedures to better the chances of the admissibility of electronic evidence. This study establishes how electronic evidence should be gathered, stored and analysed by the forensic accountant in order to be admissible legal proceedings.

Lastly, this study aims to determine how the UNCITRAL model, on which the *Electronic Communications and Transactions Act 25 of 2002* has been based, compares to the act (25 of 2002) itself. The legislation addressing electronic evidence in Canada and Australia is also considered.

Opsomming

Die studie handel oor die toelaatbaarheid van elektroniese getuienis tydens forensiese rekeningkundige ondersoeke. Elektroniese getuienis is problematies vir die forensiese rekenmeester deurdat howe dit moeilik vind om elektroniese getuienis toe te laat tydens verrigtinge. Die navorsingsmetode wat gebruik word in die studie is ’n literatuurstudie of literatuuroorsig.

Die studie poog eerstens om die forensiese rekenmeester te definieer. Die noodsaaklikheid van die forensiese rekenmeester word vasgestel. Die forensiese rekenmeester word ook gedefinieer, assok die rol en verantwoordelikhede van die forensiese rekenmeester. Die studie poog verder om vas te stel hoe die forensiese rekenmeester in Suid-Afrika gereguleer word.

Tweedens, poog die studie om ’n historiese oorsig te voorsien van wetgewing in Suid-Afrika wat elektroniese getuienis aanspreek. Wetgewing wat van toepassing is, is die *Wet op Elektroniese Kommunikasie en Transaksies 25 van 2002*, die *Strafproseswet 51 van 1977*, die *Wysigingswet op die Bewysreg 45 van 1988*, die *Wet op Bewysleer in Siviele Sake 25 van 1965* en die herroepte *Wet op Rekenaargetuienis 57 van 1983*.

Om die uitdagings wat met elektroniese getuienis gepaard gaan vas te stel, is dit krities om te verstaan hoe elektroniese getuienis ingevolge die tradisionele soorte getuienis geklassifiseer word. Dokumentêre getuienis, reële getuienis en getuienis as die produk van ’n apparaat, met spesifieke verwysing na elektroniese getuienis, word in die studie bespreek.

Hoorsêgetuienis, die oorspronklikheid van elektroniese getuienis, asook die egtheid en die betroubaarheid van elektroniese getuienis beïnvloed die toelaatbaarheid van elektroniese getuienis. Die impak van wetgewing op dié uitdagings word ook oorweeg.

Die problematiese aard van elektroniese getuienis skep reeds uitdagings tydens regsgedinge. Die forensiese rekenmeester kan sekere stappe en prosedures volg om die kans op toelaatbaarheid van elektroniese getuienis tydens regsgedinge te verbeter. Die studie bepaal hoe elektroniese getuienis deur die forensiese rekenmeester ingesamel, gestoor en geanaliseer moet word om sodoende die elektroniese getuienis tydens regsgedinge te gebruik.

Laastens bepaal die studie hoe die UNCITRAL model wet, waarop die *Wet op Elektroniese Kommunikasie en Transaksies 25 van 2002* gebaseer is, met die wet (25 van 2002*)* vergelyk. Kanadese en Australiese se wetgewing wat elektroniese getuienis aanspreek, word ook oorweeg.

List of abbreviations

ACFE	The Association of Certified Fraud Examiners
APCO	The Association of Chief Police Officers
CFE	Certified Fraud Examiner
EDRM	The Electronic Discovery Reference Model
ICFP	The Institute of Commercial Forensic Practitioners
NIFA	Network of Independent Forensic Investigators
SALRC	South African Law Reform Commission
ULCC	Uniform Law Conference of Canada
UNCITRAL	United Nations Commission on International Trade Law

Contents

1. CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1 Keywords

Admissibility, electronic evidence, documentary evidence, Electronic Communications and Transactions Act (25 of 2002), electronic evidence, forensic accountant, investigation, legislation, real evidence.

1.2 Introduction

We live in the electronic era, we therefore communicate by email, we do our banking through the internet and even business and accounting records are drafted and saved electronically (Van Rooyen, 2004:162). As a result of this electronic reliance, we are dependent on our computers, smart phones and other electronic media.

At the end of 2010, approximately 111 million people in Africa and approximately 1.97 billion people worldwide had access to and were using the internet (South African Crime Bureau, 2011). This shows that electronic media forms an integral part of our daily lives. Crimes, using computers, also have no boundaries; in other words, an American can commit a crime in South Africa without even being in South Africa.

It is clear that we use computers and the internet for practically everything, but so do modern criminals. It is thus important to know how these modern criminals commit crimes and also how to prosecute them and to make sure that they are found guilty. This can only be done once the electronic evidence of their alleged crimes is admissible in a court of law.

Forensic accounting is used during an investigation for collecting, sorting, recording and verifying evidence to be used in legal disputes (Crumbley *et al.*, 2007:4). A forensic accountant is someone who examines policies, documents and other financial information in order to detect crime or financial losses (Van Rooyen, 2004:7).

According to KMPG's forensic technology department, forensic accountants are starting to become essential to detect crimes. Their services include forensic investigations into fraud and corruption, the collection and analysis of electronic evidence and the collection and storage of evidence for civil and criminal cases (KMPG, 2013).

Traditionally, the forensic accountant assisted in investigations and collected physical evidence, such as documents and financial records. Today, however, the gathering of electronic evidence has become another important aspect of forensic investigations (CCS

South Africa, 2008-2009). The forensic accountant may be responsible for imaging computer hard drives, data recovery of deleted files, recovering of sensitive data before it can be damaged, link analysis and analysing computers or networks in order to find information relating to fraudulent transactions or other crimes (CCS South Africa, 2008-2009).

Section 5(c) of the *Police Act (7 of 1958)* determines that the South African Police Service is responsible for investigating crimes (Van Rooyen, 2004:33). This however does not mean that only the South African Police Service can investigate crimes. In *S v Botha (1995)*, Myburgh J stated that the law does not forbid anyone, who is not a member of the South African Police Service, to investigate a crime. The judge stated the following (*S v Botha and others 1995 2 SACR 598 W*):

> Society has become so specialized and there are so many laws and activities that need to be administered and regulated, that no police service can investigate and prevent all crime in a modern society without the help of private investigators.

Chapter 12 of the *Electronic Communications and Transactions Act (25 of 2002)* provides for the appointment of cyber investigators by the Director General of the Department of Communications to ensure that citizens comply with the act. The South African Police Service has the authority to appoint forensic accountants from the business sector (Mason, 2007:484). The problem is that companies sometimes initiate their own investigations and only after they have investigated the crime or losses, the complete investigation is handed to the police (Van Rooyen, 2004:3). In other words, companies perform the investigation without necessarily having a mandate from the police.

Section 21(2) of the *Criminal Procedure Act (51 of 1977)* states that "a search warrant issued under ss(1) shall require a police official to seize the article in question and shall to that end authorize such police official to search". Motata J referred to section 21(2) of the *Criminal Procedure Act (51 of 1977)* in the judgment of *Extra Dimension and others v Kruger NO and others 2004 (2) SACR 493 (T)* and concluded that it was clear that only police officers could be authorised to search and not private persons, even if they are named in the search warrant.

Another challenge regarding the gathering of electronic evidence is the search warrants. Warrants should specify the items that can be seized and these may only be items that are relevant to the case. In *Beheersmaatschappij Helling I NV and others v Magistrate,*

Cape Town, and Others 2007 (1) SACR 99 (C) the police seized all the computers including the central processing units, hard drives and computer discs. They also imaged a computer hard drive on the scene. Not all the information on the computers, hard drives and other computer media was relevant to the case and the judge ruled that the warrants were therefore unlawful and invalid.

Electronic evidence can be divided into three categories (Mason, 2007:xiii)

i. Documents or files that contain content have been written or created by one or more people. Examples include email messages and word documents. In other words, the evidence is documentary evidence.
ii. Records that have been generated by a computer and where there is no human intervention or input. Examples include data logs and ATM transactions. This evidence is thus evidence generated by a computer, device or instrument.
iii. Records that consist of both inputs generated by a computer and human inputs. Examples include financial spreadsheets, where the information is captured by a person but the computer calculates amounts and even financial statements by using the information.

The best opportunity for electronic evidence to be admissible in courts is for the evidence to be gathered, stored and presented in a capable and skilful manner (Schwikkard & Van der Merwe, 2009:450). These procedures include the chain of custody, because electronic evidence is easy to alter (Mason, 2007:51). The chain of custody refers to the safekeeping of evidence (Van Rooyen, 2004:12). This demonstrates the integrity of the evidence. Another reason for the chain of custody to be done correctly is that there should be a link between the original hardware of the computer and the digital evidence that has been imaged by the forensic accountant and presented in court as evidence (Mason, 2007:51).

Traditionally, the courts did not have much discretion regarding the admissibility of electronic evidence. The admissibility was limited to the same requirements for documentary and hearsay evidence (Schwikkard & Van der Merwe, 2009:443). Challenges, such as authenticity, originality, reliability and hearsay are prominent. (Schutte, 2009:110-111). In order for electronic evidence in the form of a computer printout to be admissible, it has to be identified by the author or a witness to prove its authenticity (Schmidt & Rademeyer, 1989:339-340). The challenge with electronic evidence is that the author is not always known and the documents are compiled from

other documents (Schutte, 2009:110). When the evidential value of evidence depends on the reliability of someone who is not testifying, it is hearsay. Thus electronic evidence will, in most cases, be hearsay evidence, and will therefore be unreliable (Schutte, 2009:110-111).

Even though the *Electronic Communications and Transactions Act (25 of 2002)* replaced the *Computer Evidence Act (57 of 1983)*, and is currently the only legislation specifically addressing electronic evidence in South Africa, challenges, such as hearsay still occur because the author or the person responsible should still be available to testify and be cross-examined. If this is not possible, the rules of hearsay still apply. (Mason, 2007: 466). There is also other legislation, which addresses electronic evidence, such as section 3 of the amended *Law of Evidence Act (45 of 1988)*, the *Civil Proceedings Evidence Act (25 of 1965)* and the *Criminal Procedure Act (51 of 1977)* (Schmidt & Rademeyer, 1989:367-368).

In order to assess whether the *Electronic Communications and Transactions Act (25 of 2002)* is most sufficient legislation in South Africa, and whether it achieves its goal, it is important to compare it to foreign legislation. Firstly, the *Electronic Communications and Transactions Act (25 of 2002)* is based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce with Guide to Enactment (1996). Countries, such as Australia, the United Kingdom, the United States of America and Canada are therefore important because they also comply with the rules of the Model Law (University of Cape Town & University of Stellenbosch, 286-288).

1.3 Problem statement

Even though law enforcement is aware of economic crimes, it has been found to lack the knowledge and training to successfully deal with economic crimes (Manning, 2005:v*).* This inability of law enforcement to deal with forensic accounting investigations has lead companies to appoint forensic accountants instead of calling the police to deal with irregularities and to investigate economic crimes, such as corruption and fraud (Van Rooyen, 2004:1).

The role of the forensic accountant dealing with electronic evidence is evident in the collection and storage of electronic evidence. We live in the era of the computer and the internet. Our legislation should thus also be applicable is this electronic era. However,

legislation has many problems with the discovery, disclosure and admissibility of electronic evidence (Schwikkard & Van der Merwe, 2009:450).

Detailed procedures for gathering and storing electronic evidence are lacking in South Africa, therefore it is difficult for South African law to be fully applicable and effective (Mason, 2005:485). In the Mashiyi case, the court made the following statement relating to electronic evidence "… that these lacunae in our law be filled and for new legislation relating specifically to electronic evidence in criminal cases be considered" (*S v Mashiyi 2002 (2) SASV 387 (Tk)*).

It is clear from the above discussion that our legislation does not always permit our courts to handle electronic evidence effectively. The question is then: what is the relevance of electronic evidence to forensic accounting investigations and how should it be gathered. Preserved and analysed to prove effective as evidence in subsequent court proceedings?

In order to answer the main question, the following secondary questions should also be answered:

i. What is a forensic accountant?
ii. How did the legislation regarding electronic evidence develop?
iii. What is considered to be electronic evidence?
iv. What are the procedures for collecting, storing and presenting electronic evidence?
v. What are the issues facing the use of electronic evidence?
vi. How does South African legislation compare to international legislation?

1.4 Research objectives

The primary objective of the research will be to establish what the impact of electronic evidence is during forensic accounting investigations.

In order to reach the primary objective, there need to be secondary objectives. The secondary objectives during the research of the subject include the following:

i. Determine an overview of the forensic accountant;
ii. Establish a historical overview of the development of legislation addressing electronic evidence;
iii. Analyse the procedures for collecting, storing and presenting electronic evidence;

iv. Establish evidence that can be considered electronic evidence;
v. Determine the issues facing the use of electronic evidence; and
vi. Compare South African legislation with international legislation.

1.5 Research methodology

This study is a literature study, focussing on the analysis of legislation as well as textual criticism. This means that existing resources on the subject will be used, and through this an opinion will be formed. The scope of the research falls within South African law. A comparative analyses of South African legislation and International law and some foreign law will also be made. Resources that will be used are legislation, case law, books, published articles and the Internet.

1.6 Chapters

Chapter 1: Introduction and background

This chapter includes an introduction to the study, a motivation for the study, the problem statement, research methodology, research questions and objectives.

Chapter 2: The forensic accountant

This chapter will aim to analyse the forensic accountant and to determine what the duties and responsibilities of the forensic accountant are relating to electronic evidence. Case law relating to forensic accountants doing investigations and dealing with electronic evidence is also important.

Chapter 3: Historical overview of the development of legislation that influenced electronic evidence

This chapter aims to provide an overview of all the legislation in South Africa that address electronic evidence and how the legislation developed.

Chapter 4: Electronic evidence

This chapter includes the various ways in which the legislation interprets electronic evidence and it includes documentary evidence, evidence by means of an apparatus and real evidence. The type of evidence needs to be established, in order to establish whether the evidence is admissible.

Chapter 5: Issues facing electronic evidence

Electronic evidence faces challenges, such as hearsay, authenticity, originality, reliability and jurisdiction. It is important to understand these challenges in order to overcome them in legislation and in doing so, to permit our courts to better address electronic evidence.

Chapter 6: The collection and storing of electronic evidence

This chapter aims to provide guidelines on how electronic evidence is to be collected and stored in practice, in order to ensure its admissibility in a court of law.

Chapter 7: International instruments and foreign law

In this chapter South African legislation will be compared with international legislation that is also based on the UNCITRAL Model Law, such as that of Australia and Canada.

Chapter 8: Conclusion

This chapter includes a summary of the research. It also includes conclusions drawn from the research and makes recommendations.

2. CHAPTER 2: THE FORENSIC ACCOUNTANT

2.1 Introduction

As the number of cases relating to electronic evidence is on the increase, the need for specialised individuals assisting in such investigations is also increasing. The forensic accountant needs to be aware of the different types of legislation and how such legislation will impact forensic accounting investigations in order to ensure or better the chances of admissibility in a court of law.

This chapter aims to provide an overview of what a forensic accountant is, as well as of the roles the forensic accountant can and may play during a forensic accounting investigation.

2.2 The need for a forensic accountant

Across the world and specifically in South Africa, crime rates are increasing, expanding from violent crimes to white-collar crime. During November 2003, at a white-collar Crime summit, the then Minister of Justice, Penuell Maduna, stated that the South African economy was suffering losses between R50 billion and R150 billion per year due to white-collar crime. He further stated that approximately 82% of South African businesses have fallen victim to white-collar crimes (Van Rooyen, 2004:1). Former judge, Willem Heath, stated that the loss South Africa was experiencing due to white-collar crimes was closer to R150 billion a year (Van Rooyen, 2004:1).

Worldwide, law enforcement has come to the realisation that to solve economic crimes, financial information is necessary. Law enforcement, however, does not have the technical skills and knowledge to effectively deal with technical and financial information (Manning, 2004:515). Case law also highlights the need for the specialised services of private investigators. In *S v Botha (1995)*, the investigation was performed by private investigators from Eskom. The defence argued that the private investigators acted beyond their powers as only the South African Police Service has the mandate to investigate crimes in terms of section 215(b) of the *Constitution of the Republic of South Africa (1996)*. Myburgh J stated that the law does not forbid anyone who is not a member of the South African Police Service to investigate a crime. He added that recently many private institutions carried out their own investigation and only handed over the results of

the investigation to the South African Police Service. Myburgh J made the following comment (*S v Botha and others 1995 2 SACR 598 W)*:

> Society has become so specialized and there are so many laws and activities that need to be administered and regulated that no police service can investigate and prevent all crime in a modern society without the help of private investigators.

Recent articles have also emphasised the need for forensic accountants. Levine *et al.,* (2002) summarise the need for forensic accountants as follows:

> Not since gangster Al Capone was nabbed for tax evasion have forensic investigators been so squarely in the public eye. The bloodhounds of bookkeeping sniff out fraud and criminal transactions in corporate financial records. And they're now blessed with expanded opportunities. Business losses in a slow economy and the recent spate of corporate collapses--think Enron--have executives scurrying to hire forensic investigators to prevent and investigate money-sucking crimes, and prepare for court cases.

It is evident that in recent times the need for the forensic accountant with information technology skills has been increasing. The "paperless office" has been on the increase as have electronic programs that store and process data. "The field of computer forensics and electronic discovery is the single fastest growing niche in forensic accounting" (Brad Sargant, 2013).

The specialised nature of technology and the significant losses experienced due to fraud and other white-collar crimes highlights the need for specialised forensic accountants. It is therefore essential to know what a forensic accountant is and how the profession is regulated in South Africa.

2.3 The definition of a forensic accountant

Multiple terms can be used to describe the individual performing an investigation of a financial nature and may include "fraud examiner, fraud auditor; forensic auditor; fraud investigator; financial crime investigator*"* (Van Romburgh, 2008:21-22).

The term "forensic" consists of two components:

i. "...courts of law, juristic or court directed and relating to the application of science to decide questions arising from crime or litigation"; and

ii. "...includes the function of examination or analysing" (Van Rooyen, 2004:7).

According to the Network of Independent Forensic Investigators (2011) forensic accounting is the use of accounting and audit knowledge and experience combined with investigation skills. A forensic accountant will review financial information and other supporting documentation and prepare a report to present the findings in a report that may be used in criminal proceedings (NIFA, 2011).

According to the Canadian Institute of Chartered Investigators (2013), investigative and forensic accounting engagements "require the application of professional accounting skills, investigative skills, and an investigative mind set, and involve disputes or anticipated disputes, or engagements where there are risks, concerns of allegations of fraud or other illegal or unethical conduct".

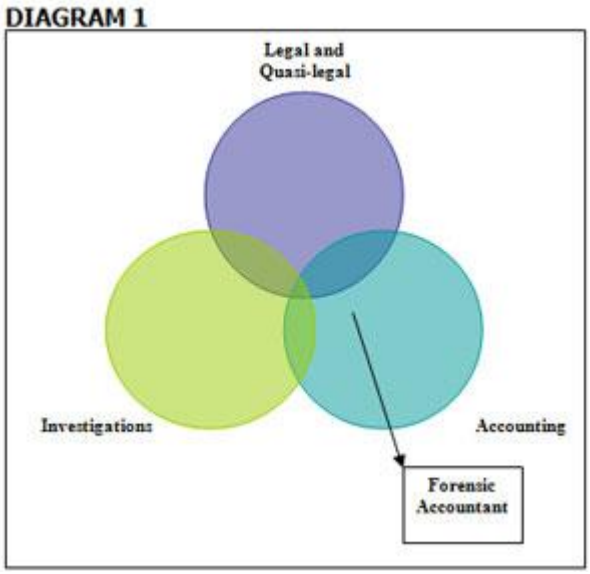
According to the Association of Certified Fraud Examiners (ACFE), a forensic accountant plays an important role in the investigation of crimes, such as fraud and corruption and consequently in civil and criminal proceedings. The forensic accountant will use accounting and investigative knowledge to assist in investigations and during litigation (ACFE, 2013).

According to KPMG (2013), a forensic investigation occurs "when suspicions of fraud, or bribery and corruption, or financial misconduct and mismanagement surface, specialist independent investigation, support and advice are required to quickly and effectively deal with these issues".

Even though the forensic accountant may not assume the rights and duties of a police officer, he/she should embrace the skills required of both the police officer and the accountant. An accountant analyses books and records and uses his/her knowledge to testify as a forensic accountant in court. The police officer can conduct interviews, analyse evidence and is familiar with the applicable laws (Manning, 2004:515).

The skills of the forensic accountant can be illustrated as follows (Van Romburgh, 2008:31):

Figure 1



Source: Accountancy SA. Defining the South African Forensic Accountant

By utilising all the different definitions of the forensic accountant, the basic skill set of the forensic accountant can be summarised as follows

i. Legal knowledge in both civil and criminal proceedings;

ii. Accounting knowledge;

iii. Investigative skills;

iv. Interviewing skills;

v. Information technology and data analytic skills; and

vi. The ability to testify during legal proceedings.

2.4 Roles of a forensic accountant

To understand the roles of the forensic accountant, it is critical to understand the services a forensic accountant can render.

The forensic accountant's focus area includes investigating the following economic and/or white-collar crimes:

i. Theft;

ii. Asset misappropriation;

iii. Financial misrepresentation;

iv. Embezzlement;

v. Corruption, bribery, racketeering and extortion; and

vi. Money laundering (Van Romburgh, 2008:16-17).

In recent times, the use of forensic accountants in legal proceedings has been on the increase. During the Shaik case, KPMG's Johan van der Walt testified as an expert witness with regard to the forensic investigation conducted. Squires J made the following comment regarding the purpose of the forensic investigation (*S v Shaik and others [2005] 3 All SA 211 (D))*:

> Van der Walt was plainly an impartial witness who simply described chapter and verse, in extraordinary detail, the evidence that he culled from the mass of documents given to him to investigate. In the one or two respects that he expressed an opinion, there was nothing amiss about so doing, but we have not relied on any of those.

In order to determine the services of the forensic accountant, one can look at the market leaders in the industry, which are the "big four" auditing firms internationally, namely:

i. Ernest & Young;

ii. KPMG;

iii. PricewaterhouseCoopers; and

iv. Deloitte.

2.4.1 Ernest & Young

Ernest & Young's Fraud Investigation and Dispute Services Division states that they investigate unusual financial activities, perform evidence recovery and review financial documentation. The specific services the Fraud and Investigation and Dispute Services Division render include the following (EY, 2013):

v. Anti-fraud;

vi. Corporate Compliance;

vii. Dispute Services;

viii. Forensic Technology and Discovery Services; and

ix. Fraud Investigations.

2.4.2 KPMG

KPMG's Forensic Department provides the following services: "...establish the facts, collect and preserve evidence, assist recoveries and lay a foundation for criminal or civil action. We can also deploy technology tools to help clients deal effectively with large amounts of data and documentation, to manage and disclose important material or highlight fraud, weaknesses and business opportunities from within the corporate data" (KPMG, 2013).

KPMG's (2013) services further include the following:

i. Corporate Intelligence Services;

ii. Dispute Advisory Services;

iii. Forensic Technology;

iv. Fraud Risk Management;

v. KPMG Ethics and Fraud Hotline;

vi. Investigations; and

vii. Regulatory Compliance Monitoring.

KPMG's Forensic Technology Division specifically deals with electronic evidence. The services that the Forensic Technology Division renders are as follow (KPMG, 2013):

i. "Computer forensics;

ii. Digital evidence acquisition and analysis;

iii. Forensic data analysis;

iv. Proactive forensic data analysis: K-Trace;

v. EMA forensic data centre;

vi. E-discovery;

vii. Project management of the process from data recovery through to discovery;

viii. Recovery and analysis of digital material;

ix. Recovery and analysis of traditional paper-based material;

x. Intelligent data processing, including the elimination of duplication and the extractions of metadata;

xi. Facilities for identification and review of key documents; and

xii. Preparation and delivery of court bundles."

2.4.3 PricewaterhouseCoopers

The Forensic Investigations and Dispute Resolution Division of PricewaterhouseCoopers renders the following services (PWC, 2013):

i. Forensic investigations;

ii. Forensic accounting and financial analyses;

iii. Advanced technology;

iv. Dispute resolutions; and

v. Quantifying claims in the commercial, transaction, intellectual, competition and environmental disputes.

2.4.4 Deloitte

Deloitte's Forensic division includes individuals such as forensic accountants, legal specialists, law enforcement specialists and business intelligence specialists. They also utilise "state-of-the-art forensic technology". Deloitte's services include the following (Deloite, 2013):

i. Advisory and solutions;

ii. "Forensic Data Analytics;

iii. Deloitte Discovery;

iv. Investigations;

v. Financial crimes;

vi. Tip-Offs Anonymous".

Deloitte's discovery team collects, stores and examines data as part of a discovery process or to potentially use the data as evidence during legal proceedings (Deloitte, 2013).

2.5 The regulation of the South African forensic accountant

2.5.1 The Institute of Commercial Forensic Practitioners

Currently there is only one South African regulatory body that regulates forensic accountants, namely the Institute of Commercial Forensic Practitioners (ICFP). The ICFP was only recently established (ICFP, 2011). Even though the ICFP is not a government regulated body, it is a self-regulated body.

The first step towards the establishment of the ICFP occurred in August 2007, when key role players in the forensic industry met to discuss the regulation of the forensic industry. Role players included (Van Romburgh, 2008:18):

i. Forensic Divisions of the big four auditing firms;

ii. Prominent medium-sized forensic firms;

iii. Prominent academics in the field of forensic accounting;

iv. Life insurance industry;

v. Major banks;

vi. Forensic divisions of prominent legal firms;

vii. The Special Investigating Unit;

viii. The Auditor General;

ix. South African Revenue Services;

x. National Prosecuting Authority;

xi. Sasol; and

xii. Prominent individuals like Advocate Jan Henning..

As a result, the ICFP was established. The ICFP's mission is to *"Cohere, Co-ordinate and Self-regulate"* the forensic industry in South Africa. The ICPF states that it aims to (ICFP, 2011):

i. "cohere the emerging industry in South Africa,
ii. co-ordinate key initiatives to develop the industry,
iii. serve the interests of the Commercial Forensic Practitioners and society, by upholding internationally acceptable professional standards and integrity, and the pre-eminence of South African Commercial Forensic Practitioners nationally and internationally,
iv. Delivering competent entry level members with relevant skills,
v. Providing services to assist members to maintain and enhance their professional competence thereby enabling them to create value for their clients and employers,
vi. Enhancing the quality of information used in the private and public sectors for measuring and enhancing organisational performance in relation to commercial forensic matters,
vii. Running and facilitating programmes to transform the profession and to facilitate community upliftment,
viii. Fulfilling a leadership role regarding relevant business related issues and providing reliable and respected public commentary, and

ix. Influence stakeholders through improving their confidence in ICFP and its members."

2.5.2 The Association of Certified Fraud Examiners

The Association of Certified Fraud Examiners ("ACFE") is the largest anti-fraud institution in the world. As of 2013, the ACFE had more than 65 000 members worldwide. The ACFE provides anti-fraud training and education. The ACFE provides members with the Certified Fraud Examiner (CFE) accreditation (ACFE, 2014).

The ACFE has a South African chapter. The ACFE South Africa is registered by the South African Qualifications Authority and affords a professional status to individuals with the CFE qualification as per the National Qualifications Framework Act 67 of 2008 (AFCE SA, 2014).

The mission of the ACFE South Africa is to reduce instances of fraud and white-collar crime and also to assist with fraud detection and prevention (AFCE SA, 2014). To accomplish its mission, the ACFE:

i. "Provides bona fide qualifications for Certified Fraud Examiners through administration of the CFE Examination and the Leadership: Certified Forensic Practitioner.
ii. Sets high standards for admission, including demonstrated competence through mandatory continuing professional education.
iii. Requires members to adhere to a strict code of professional conduct and ethics.
iv. Serves as the international representative for Certified Fraud Examiners to business, government and academic institutions.
v. Provides leadership to inspire public confidence in the integrity, objectivity, and professionalism of Certified Fraud Examiners."

The CFE accreditation is recognised not only locally, but also internationally. The designation is recognised by the government and courts, as well as academic institutions. Furthermore, most companies recognised the CFE accreditation as the premier qualification (ACFE SA, 2014).

2.5.3 Other

Forensic accountants can also be registered with other accounting or auditing regulatory bodies in South Africa. These bodies, however, do not regulate the forensic industry and members must comply with the necessary requirements. Such bodies include:

i. The South African Institute of Chartered Accountants (SAICA 2008);
ii. The South African Institute of Professional Accountants (SAIPA 2014);
iii. The Chartered Institute of Management Accountants (CIMA SA, 2014); and
iv. The South African Institute of Government Auditors (SAIGA, 2014).

2.6 Conclusion

It is evident that the need for certified forensic investigators is on the increase, not only for the profession itself but also for the future prosecution of criminals. In recent years, the services of the forensic accountant have become more extensive and include services relating to electronic media and evidence. In the article *"Careers to count on"*, the forensic accounting profession was identified as one the of the most secure career tracks in the United States of America (Levine *et al.,* 2002).

3. CHAPTER 3: HISTORICAL DEVELOPMENT OF LEGISLATION THAT INFLUENCED ELECTRONIC EVIDENCE

3.1 Introduction

This chapter aims to provide a brief historical overview of relevant South African law dealing with electronic evidence. The technological advances over the past few decades have impacted significantly on the admissibility of electronic evidence. This chapter focuses on how the relevant legislation was developed to deal with these technological advances. In the technological era that we live in, our law has to adapt to the changing environment. In order to address the issues facing electronic evidence, one needs to understand the legislation that governs such evidence.

3.2 The Civil Proceedings Evidence Act (25 of 1965)

The *Civil Proceedings Evidence Act (25 of 1965)* was assented to on 15 March 1965 and commenced on 30 June 1967. The main purpose, according to the long title of the act, is to state the law of evidence in regard to civil proceedings and to provide for "other incidental matters". This act provides *inter alia* for the admissibility of evidence, documentary evidence and also the sufficiency of evidence.

An important relaxation of the hearsay rule was made through the *Civil Proceedings Evidence Act (25 of 1965)*. Initially the act was only applicable to civil cases, but this restriction was lifted by section 222 of the *Criminal Procedure Act (51 of 1977)*, which makes the provisions of sections 33 to 38 of the *Civil Proceedings Evidence Act (25 of 1965)*, relating to documentary evidence, applicable to criminal proceedings (Schmidt & Rademeyer 1989:495). Section 33 of the *Civil Proceedings Evidence Act (25 of 1966)* defines a document as any "book, map, drawing or photograph" and a statement as a representation of facts, in words or by other means.

Section 34(1) of the *Civil Proceedings Evidence Act (25 of 1965)* states that in instances where oral evidence would be admissible in a civil case, a statement made by an individual, in the form of a document, would also be admissible if the original document is submitted. The act however provides two requirements for this admissibility. Firstly, the individual who made the statement had to have personal knowledge of the matter discussed in the statement. Otherwise, the document must form part of a continuous record and the individual who made the statement did so in execution his/her duties.

Such individual was supplied with information by an individual who had or was supposed to have personal knowledge of the matters dealt with in the statement.

Section 34(1)(b) of the the *Civil Proceedings Evidence Act (25 of 1965)* further stipulates that the individual who made the statement is to be called as a witness during the proceedings, with the following exceptions:

i. If the individual is dead;

ii. If the individual is unfit due to a bodily or mental condition to attend the proceeding;

iii. If the individual is outside of the Republic of South Africa and it is not reasonably practical for the individual to attend the proceedings; or

iv. All reasonable efforts have been made to locate the individual without any success.

Shortcomings in South Africa's law of evidence with regard to electronic evidence first came to light in 1976 in the case of *Narlis v South African Bank of Athens 1976 2 SA 573 (A) 577H* (Schwikkard & Van der Merwe, 2009:443). The court ruled that "a computer, perhaps fortunately, is not a person" and therefore a computer printout was not allowed in terms of the *Civil Proceedings Evidence Act (25 of 1965)* (*Narlis v South African Bank of Athens 1976 2 SA 573 (A) 577H.)* Due to the concerns that were raised after electronic evidence was not allowed in *Narlis v South African Bank of Athens 1976 2 SA 573 (A) 577H,* the South African Law Commission was approached to investigate the need for specific legislation for electronic evidence. The Commission ruled that an amendment to section 34 of the *Civil Proceedings Evidence Act (25 of 1965)* would not have been sufficient to solve the challenges with regard to electronic evidence (Schwikkard & Van der Merwe, 2009:444). Hence, the *Computer Evidence Act (57 of 1983)* was introduced in civil cases (Schwikkard & Van der Merwe, 2009:444).

3.3 The Criminal Procedure Act (51 of 1977)

The *Criminal Procedure Act (51 of 1977)* repealed and replaced the *Criminal Procedure Act (56 of 1955)*. The *Criminal Procedure Act (51 of 1977)* was assented to on 21 April 1977 and commenced on 22 July 1977. The purpose of the *Act (51 of 1977)* is to make provision for procedures and related matters in criminal proceedings.

The courts' approach with regard to the admissibility of electronic evidence in criminal cases is based on section 221 and section 236 of the *Criminal Procedure Act (51 of 1977)* (Schwikkard & Van der Merwe, 2009:445).

Section 221 of the *Criminal Procedure Act (51 of 1977)* provides for the admissibility of electronic evidence in the form of a document, i.e. certain trade documents and business records. The relevant document, however, has to prove the content thereof. Furthermore, it must have been compiled during the ordinary course of business by a person who has personal knowledge of the facts contained in the document (Schmidt & Rademeyer, 1989:367). Section 221(1) (b) of the *Criminal Procedure Act (51 of 1977)* states that the information has to be furnished by an individual who has personal knowledge of the facts in the document, with the following exceptions (Bellengère *et al.*, 2013:75):

i. when the individual is dead;

ii. when the individual is outside of the Republic of South Africa;

iii. due to his/her physical or mental condition, the individual is incapable of appearing as a witness;

iv. when the individual cannot be identified or found with reasonable soundness; and

v. considering the time lapsed, as well as other circumstances, it cannot be expected of the individual to remember the facts contained in the document.

Based on section 221(5) of the *Criminal Procedure Act (51 of 1977)*, the word "document" also includes an apparatus through which information can be stored and recorded. This meaning of the word "document" was considered in the case of *S v Harper 1981 (1) SA 88 (D)* (Schwikkard & Van der Merwe, 2009:445). When the question was asked if computer printouts are documents, Milne J stated the following:

> If the computer printouts...are 'documents' within the ordinary grammatical meaning of that word, then they are admissible, if they are not, then, in my view they are inadmissible...Computers do record and store information but they do a great deal else; inter alia, they sort and collate information and make adjustments...The extended definition of 'document' is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than the mere storage or recording of information.

Therefore, computer printouts of computers that merely stored the information will be subject to this section of the *Criminal Procedure Act (51 of 1977)*. If the computer had any active function over and above the storage of the information, the computer printouts will be inadmissible in terms of the *Criminal Procedure Act (51 of 1977)* (Schwikkard & Van der Merwe, 2009:446).

The findings of *S v Harper 1981 (1) SA 88 (D)* were later used in *S v Mashiyi 2002 (2) SASV 387 (Tk)*. It was also concluded that the definition of the word "document" as in section 221 of the *Criminal Procedure Act (51 of 1977)* excluded computer printouts, because the printouts contained information that was "obtained after treatment by arrangement, sorting, synthesis and calculation by the computer" (*S v Mashiyi 2002 (2) SASV 387 (Tk)*).

Section 236 of the *Criminal Procedure Act (51 of 1977)* provides for the proof of entries of accounting and banking records. Based on this section, a "document" is also a recording or a transcribed computer printout generated by any mechanical or electronic apparatus and any apparatus that stores or records information (Zeffertt *et al.*, 2003:693). The requirements of this section are as follows:

i. an affidavit should be sworn by an individual that was in service of the specific bank;

ii. that the said accounting records are from the intended bank;

iii. that the said accounting entries were made during the normal course of business; and

iv. that the said accounting records or document was stored by and under the control of the said bank.

3.4 The Computer Evidence Act (57 of 1983) (repealed)

The *Computer Evidence Act (57 of 1983)* (now repealed) determined that a certified computer printout was admissible if the facts contained in the computer printout would have been admissible if tendered as direct, oral evidence (Schwikkard & Van der Merwe, 2009:444). A computer printout can be certified by means of an affidavit:

i. That identifies the computer printout and any copies thereof;

ii. That describes the nature, the extent, the sources of the data and instructions, as well as the purpose and effect of the processed data;

iii. That certifies that the computer was fully functional; and

iv. That there are no reasons to doubt the reliability of the information contained in the computer printout (Schmidt & Rademeyer, 1989:368).

The court may attach as much or little evidential value to the computer printout as prescribed by the circumstances of the case (Schwikkard & Van der Merwe, 2009:444). The *Computer Evidence Act (57 of 1983)* required that a deponent had to be a competent individual; firstly, because of his/her knowledge and experience with computers; and secondly, with regard to his/her investigation into the facts and the workings of the computer and the data (Schwikkard & Van der Merwe, 2009:444).

Challenges were experienced with the compliance of the *Computer Evidence Act (57 of 1983)* due to the excessive technical requirements (Schwikkard & Van der Merwe, 2009:445). In the case of *Ex parte Rosch [1998] 1 All SA 319 (W)* two sets of evidence were submitted.

i. The first set of documents was copies of a hotel's telephone invoices. The respondent relied on the fact that only the original documents could be relied upon. The court found that the individual who created the documents could not, after all reasonable efforts, be determined. The court allowed for the documents to be admitted as evidence during the proceedings as the telephone operator recorded the information in performing his duties.

ii. The second set of documents consisted of a telephone company's records which were computer printouts that were automatically generated when calls were made by subscribers. The documents were created by a computer and with no human

input. The court stated that the documents could not be admitted through the provisions of section 34(1) of the *Civil Proceedings Evidence Act (25 of 1965)*, as the statement was not made by a person, but in all essence by a computer. The court further stated that the documents could also not be admitted through the *Computer Evidence Act (57 of 1983).* In the case of *Ex parte Rosch [1998] 1 All SA 319 (W)* no specific exclusion pertained and therefore the provisions of the *Computer Evidence Act (57 of 1983)* could not be utilised. As the documents were not created by a person, the exclusion grounds to hearsay in the *Law of Evidence Amendment Act (45 of 1988)* were also inapplicable. The court held that the computer printouts were real evidence, as they were created without human input and therefore there was no opportunity for human error or deceit.

The case of *Ex parte Rosch [1998] 1 All SA 319 (W)* illustrated the court's duty to adapt to changing technology. It further illustrated that the *Computer Evidence Act (57 of 1983)* had limitations and neither of the respondents placed any reliance on the act to admit the electronic evidence. The court held that the question that needed to be answered was if a computer printout was specifically excluded by the Computer Evidence Act (57 of 1983). The court found that: *"*In our view a reading of the statute makes it plain that the statute does not require that whatever is retrieved from a computer can be used if the statute's requirements have been met. It is a facilitating act, not a restricting one". The *Computer Evidence Act (57 of 1983)* was therefore not the solution to the issues facing electronic evidence, and the need once again arose for new legislation.

3.5 The Law of Evidence Amendment Act (45 of 1988)

The *Law of Evidence Amendment Act (45 of 1988)* was assented to 15 April 1988 and commenced on 3 October 1988. The *Law of Evidence Amendment Act (45 of 1988)* changed the law on hearsay by changing the definition of hearsay from that of the common law.

One of the biggest challenges regarding computer evidence is that it is regarded as hearsay evidence. Section 3 of the *Law of Evidence Amendment Act (45 of 1988)* grants the discretion to the courts to allow hearsay evidence in certain circumstances (Schmidt & Rademeyer, 1989:367).

Hearsay evidence is evidence of that which another person told the witness. The witness merely relays what he or she heard (Schmidt & Rademeyer, 1989: 472). Hearsay

evidence is inadmissible, because it is normally unreliable and for that reason can mislead the court. It is unreliable since the individual who observed the facts, does not testify and inform the court of his/her observations in person. Furthermore, the individual who observed the facts is not subject to the oath of the court. His or her testimony can also not be questioned under cross-examination (Schmidt & Rademeyer, 1989:472-473). Hearsay evidence is discussed in more detail in Chapter 5.

The general rule of hearsay evidence as per section 3(1) of the *Law of Evidence Amendment Act (45 of 1988)* is that hearsay is not admissible in criminal or civil proceedings, with some exceptions. The following instances will allow for hearsay evidence to be admitted:

i. If each party against whom the hearsay evidence will be submitted agrees to the admission of the hearsay evidence;

ii. If the individual on whose credibility the probative value of the hearsay evidence depends, testifies at the proceedings;

iii. If the court is of the opinion that the evidence should be admitted in the best interest of justice. The court may consider the following factors:

    - The nature of the proceedings;
    - The nature of the evidence;
    - The purpose of the evidence;
    - The probative value of the evidence;
    - Why the evidence is not provided by the individual on whose credibility the probative value of the hearsay evidence depends;
    - If the admission of the evidence might prejudice any party; and
    - Any other factor in the opinion of the court.

Hearsay evidence, in the form of a computer printout, may then be admissible if evidence can be submitted that illustrates that the information that was captured on the computer, was reasonably reliable (Schmidt & Rademeyer, 1989:367). The definition of hearsay refers to “evidence, whether oral or in writing” and therefore data messages will be included in the definition of hearsay. If the data message meets the exception criteria,

stipulated in section 3 of the *Law of Evidence Amendment Act (45 of 1988)*, and such evidence may be admissible (Mason, 2007:467-468).

Section 3(1)(c)(vii) of the *Law of Evidence Amendment Act (45 of 1988)* allows for the court to consider any factor that may be in the interest of justice to allow the hearsay evidence. The following factors may play a part in the court's decision (Schmidt & Rademeyer, 1989:367):

i. The ease of obtaining the original information;

ii. The importance of the electronic evidence;

iii. Is there any motive for the computer user to falsify information; and

iv. The defence grounds of the opponent.

The court's view should be to rather allow the evidence, because merely allowing the evidence does not mean that the evidence will carry much evidential weight (Schmidt & Rademeyer, 1989:367). When considering electronic evidence, a cautious approach forms part of assessing the admissibility. The evidential weight of evidence should, however, not be confused with the admissibility of the evidence. Old law of evidence determines that "admissibility and weight should never be blurred" (De Villiers, 2012).

3.6 The Electronic Communications and Transactions Act (25 of 2002)

The *Computer Evidence Act (57 of 1983)* was deemed to lack proper elements to deal with electronic evidence. In the Mashiyi case the following was said regarding electronic evidence (*S v Mashiyi 2002 (2) SASV 387 (Tk)*): "That these lacunae in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered".

A discussion paper on electronic commerce was launched during July 1999 by the Department of Communication. The Green Paper on electronic commerce subsequently followed during November 2000, which finally led to the development and implementation of the *Electronic Communications and Transactions Act (25 of 2002)*. Section 92 of this Act repealed the *Computer Evidence Act (57 of 1983)*.

Previous legislation would still be relevant, since provisions of the *Electronic Communications and Transactions Act (25 of 2002)* do not apply retrospective. Furthermore, the C*riminal Procedure Act (51 of 1977)* and other legislation addressing

hearsay make provision for exceptions to the hearsay rule and would therefore still be relevant and applicable (Schwikkard & Van der Merwe, 2009:443).

The *Electronic Communications and Transactions Act (25 of 2002)* moves away from the concept of "computer printouts" and focuses more on terms, such as "data" and "data messages" (Schwikkard & Van der Merwe, 2009:446). Section 1 of the *Electronic Communications and Transactions Act (25 of 2002)* defines data as "electronic representation of information in any form". Furthermore, a data message is defined as "data generated, sent, received or stored by electronic means".

The various forms, in which electronic evidence can be presented, i.e. documentary evidence, real evidence, data messages and evidence as the product of an apparatus, are discussed in detail in Chapter 4 of this study.

Section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* addresses the admissibility of data messages, as well as the evidential weight that data messages carry (Mason, 2007:463). Section 15 states that law of evidence should not deny the admissibility of data messages on the mere grounds that it is a data message. If further states that if the evidence is the best evidence that could or could reasonably be expected to be obtained, the evidence should not be denied on the grounds that it is not in its original form.

Section 15(3) of the *Electronic Communications and Transactions Act (25 of 2002)* states that when determining the evidential weight of the data message, the court should consider the reliability of how the data message was generated or stored, how the integrity of the data message was maintained, how its creator was identified and any other fact that the court deems relevant.

Section 15(4) of the *Electronic Communications and Transactions Act (25 of 2002)* states that if the data message was made by an individual in the normal course of business and a copy of a printout of such a message can be certified by an officer in the service, that that individual, the printout, record or copy will be admissible on its mere production during any legal proceedings. The evidence will furthermore be "rebuttable proof of the facts" contained in the printout or record. This wording of this section may, however, be problematic, due to the following (Mason, 2007:471-472):

i. Previously, exceptions were made for business records, this section allows for all documents and communication made in the "ordinary course of business".

Technically this would therefore apply to any email sent or received during working hours;

ii. Not all business records can be assumed to be reliable. Bank records can be considered as reliable as they are regulated by trusted institutions. As the *Electronic Communications and Transactions Act (25 of 2002)* provides for any business records, this includes business and there is no guarantee that all records are kept accurately and honestly;

iii. Section 15(4) of the *Electronic Communications and Transactions Act (25 of 2002)* also only requires a certificate by an officer in the individual's service. Previously an affidavit was required;

iv. Section 15(4) of the *Electronic Communications and Transactions Act (25 of 2002)* makes the range of evidence that can be admissible that much more and the courts could therefore be expected to consider much larger volumes of electronic evidence;

v. If this section is applied during criminal proceedings, the onus of proof is shifted to the accused due to the presumption of truth.

The impact of the aforementioned is that not only is it possible for unreliable electronic evidence to be admitted during the ordinary course of business, it furthermore has the potential to infringe on the accused's constitutional rights by shifting the onus of proof onto him/her.

Section 15(1) of the *Electronic Communications and Transactions Act (25 of 2002)* does not allow for every data message to be admissible. All data messages that constitute a document have to satisfy the documentary requirements of South African law of evidence, except where the *Electronic Communications and Transactions Act (25 of 2002)* exempts them (Mason, 2007:464). The requirements for electronic evidence as per South African law of evidence can be listed as follows and are discussed in Chapter 4 of this study:

(i) Production of a document;

(ii) Document in its original form; and

(iii) The document has to be proven as authentic (Mason, 2007:465-464).

The meaning of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* is, however, not very clear. Electronic evidence has to overcome three traditional hurdles, namely originality, authenticity and hearsay. The first hurdle, originality, is addressed by section 15(1)(b) of the *Electronic Communications and Transactions Act (25 of 2002)* provided that it is the best evidence. The question can then be asked of how section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* impacts on the hurdles of authentication and hearsay (Collier, 2005:6-9).

In *Ndlovu v Minister of Correctional Services & Another 2004 JDR 0328 (W)*, the admissibility of a computer printout was in dispute. The computer printout was in in the form of a diary, reflecting the monitoring of the parolee since his release until date of printout. The entries into the diary were made by the parole officer or a monitor. Ndlovu argued that the computer printout was not the original and as it was a computer printout the court should not allow it unless properly proved. The court analysed whether the printout should be admissible or not in terms of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)*, read in conjunction with section 3 of the *Law of Evidence Amendment Act (45 of 1988)*. The court found the printout admissible, not because of the provisions of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)*, but rather in terms of the exclusion rules applicable to hearsay in section 3 of the *Law of Evidence Amendment Act (45 of 1988)*, which allows for the court's discretion to allow hearsay evidence.

Section 15(2) of the *Electronic Communications and Transactions Act (25 of 2002)* provides for the court to determine the evidential weight the data message should carry. Section 15(3) of the *Electronic Communications and Transactions Act (25 of 2002)* prescribes methods to the court in assessing the evidential weight. These sections of the *Electronic Communications and Transactions Act (25 of 2002)* should address the hurdles of authenticity and hearsay (Collier, 2005:6-9). The court was, however, not prepared to do so in the case of Ndlovu. The court held that even though the *Electronic Communications and Transactions Act (25 of 2002)* attempts to facilitate the admissibility of electronic evidence, it does not entirely address the rules of hearsay. The court further held that all that section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* does is to exclude evidence rules that deny the admissibility of electronic evidence based on its electronic foundation. The following statement was made by the court:

> Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving the evidence, there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence. On the other hand, where the probative value of the evidence depends upon the 'credibility' of the computer (because information was processed by the computer), section 3 of the Law of Evidence Amendment Act 45 of 1988 will not apply, and there is every reason to suppose that section 15(1), read with section 15(2) and (3), intend for such 'hearsay' evidence to be admitted, and due evidential weight to be given thereto according to an assessment having due regard to certain factors.

Schwikkard and Van der Merwe (2009:448) state that the court admitted the electronic evidence without a detailed examination, on the basis that no substantial objection was made in this regard, as it was satisfied that the electronic evidence should not be excluded on the bases of authenticity and originality.

It is therefore still unclear how section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* impacts the requirement of authenticity and the hearsay rule (Collier, 2005:6-9). Schwikkard and Van der Merwe (2009:448) state that the originality requirement can be addressed by section 15(1) of the *Electronic Communications and Transactions Act (25 of 2002)* and section 15(3) of the *Electronic Communications and Transactions Act (25 of 2002)* can assist when determining the authenticity of a computer printout. The courts, however, are not always so willing.

The purpose of this study is to explore the evidentiary challenges that is associated with electronic evidence. The aforementioned questions relating to hearsay and authenticity were already evident in 2005, and to date electronic evidence still faces the same challenges (Collier, 2005:6-9). The *Electronic Communications and Transactions Act (25 of 2002)* is the most recent legislation to address electronic evidence, but still the courts would rather rely on earlier legislation that addresses documentary evidence and hearsay evidence. If the court does not place any reliance on the *Electronic Communications and Transactions Act (25 of 2002)*, then the purpose of the act should be determined.

In *S v Ndiki 2008 (2) SASV 252* the court also made the distinction, albeit *obiter dictum,* between two types of electronic evidence:

i. If the evidential value of electronic evidence depends on an individual that will not be called as a witness, then that electronic evidence would be considered as hearsay evidence; and

ii. If the evidential value of the evidence "depends solely upon the reliability and accuracy of the computer itself" such evidence constitutes real evidence.

Van Zyl J stated that the *Electronic Communications and Transactions Act (25 of 2002)* is unclear regarding whether the provisions of section 15 override the hearsay rules as in section 3 of the *Law of Evidence Amendment Act (45 of 1988)* as the *Electronic Communications and Transactions Act (25 of 2002)* does not say that it does not. He added that it would appear that the definition of "data message" in section 1 of the *Electronic Communications and Transactions Act (25 of 2002)* is broad enough to include hearsay evidence *(S v Ndiki 2008 (2) SASV 252).*

In *Ndlovu v Minister of Correctional Service and other [2006] 4 All SA 165 (W)*, Gautshi J stated that if the probative value of the electronic evidence depends on the credibility of a person, other than the person providing the evidence, then "there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence". He did, however, also add that if the probative value of the electronic evidence relies on a computer, the provisions of section 3 of the *Law of Evidence Amendment Act (45 of 1988)* would not be applicable and then there is every reason to suppose that the purpose of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* is to allow the admissibility of such hearsay evidence. Some opinions, however, differ. Others argue that if the probative value of the computer depends on a computer, there is still a person who captures the information on the computer or who enables the computer to accurately capture information. It would therefore fall under the definition of hearsay in terms of section 3(4) of the *Law of Evidence Amendment Act (45 of 1988)* (Zeffertt *et al.,* 2003:393-394). Hearsay evidence will be discussed in detail in Chapter 5 of this study.

In *S v Ndiki 2008 (2) SASV 252*, Van Zyl J stated that section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* makes provision for electronic evidence to be treated in the "same way as real evidence at common law". The court's approach to electronic evidence would therefore rather be inclusionary than exclusionary and the purpose of the court would then be to determine the evidential weight that ought to be added to the electronic evidence.

3.7 South African Law Reform Commission

The South African Law Reform Commission (SALRC) was established with the adoption of the *South African Law Reform Commission Act (19 of 1973)*. It is the objective of the SALRC to do research into South African law and in doing so, to make suggestions and recommendations to the South African Government on how to further develop the law and also how to improve the law.

3.7.1 Discussion papers

For several years the South Africa Law Reform Commission has been investigating the admissibility of computer-generated evidence. Project 95 aimed to investigate the admissibility of electronic evidence. Project 108 was launched to investigate computer-related crimes (Schwikkard & Van der Merwe, 2009:446).

In the 1997 Annual Report of the South African Law Commission, it was announced that Project 95 would be halted pending the outcome of Project 108, as there were overlaps between the two investigations.

Prior to the investigations, it was proposed that a Computer Misuse Act be developed. The proposed Computer Misuse Act proposed to address *inter alia* procedural matters, such as jurisdiction, search and seizures and the admissibility of evidence.

The proposed Computer Misuse Act submitted contained the following provision for the admissibility of computer-generated evidence:

> Notwithstanding the provisions of any law, information in any medium, including but not confined to data or computer output, shall be admissible as evidence of any fact stated therein in any criminal proceedings in terms of this Act.

The proposed act did, however, include the following provisions for the above rule:

i. If a standard or best procedure has been followed to obtain the information; and

ii. If a standard procedure was not followed, and in the opinion of the court, it does not greatly prejudice the accused, such evidence will be admissible. The court will, however, add a corresponding evidential weight to such evidence.

The proposed Computer Misuse Act was, however, never implemented. Schwikkard and Van der Merwe (2009:446) are of the opinion that this was due to the implementation of the *Electronic Communications and Transactions Act (25 of 2002)* that was published on 2 August 2002. Due to the challenges that electronic evidence currently still faces, the proposed Computer Misuse Act may be important for future legislation addressing computer-generated evidence.

3.7.2 Issue paper

Paper 27 on Project 126 was commenced in 2002 when the SALRC set out to investigate electronic evidence. Paper 27 identified the various forms of legislation that address or can be used to address electronic evidence. In the 2010/2011 Annual Report of the SALRC, it was said that Issue Paper 27 was specifically concerned with the relationship between the general hearsay rule and the provisions of section 3 of the *Electronic Communications and Transactions Act (25 of 2002).*

Paper 27 raised the *inter alia* following questions for discussion:

i. Should the *Electronic Communications and Transactions Act (25 of 2002)* be reviewed on a regular basis in order to address the advances in technology?

ii. Is the *Electronic Communications and Transactions Act (25 of 2002)* adequate to address the admissibility of electronic evidence in both criminal and civil proceedings?

iii. Should section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* state that a data message is automatically admissible as evidence and the court's only discretion would be to assess the evidential weight of the evidence?

iv. Should the *Electronic Communications and Transactions Act (25 of 2002)* clearly distinguish between electronic evidence that was generated by a computer or another device without any human input, i.e. real evidence and evidence that was generated by a computer or another device but with human intervention, i.e. hearsay evidence?

v. Are the provisions as set out in the *Electronic Communications and Transactions Act (25 of 2002)* sufficient to address the admissibility of electronic evidence in a court of law?

These questions form the basis of this study. The SALRC has, however, not published the report on this project as yet. The findings of this project will be significant and may shape legislation dealing with electronic evidence going forward.

3.8 Conclusion

Each of the pieces of legislation addresses one or more aspect of electronic evidence. The *Electronic Communications and Transactions Act (25 of 2002)* is deemed the most comprehensive legislation addressing electronic evidence. The *Electronic Communications and Transactions Act (25 of 2002)* is, however, not always as clear as it is expected to be. In some cases, courts have rather used earlier legislation providing exceptions for hearsay, to admit electronic evidence as opposed to the *Electronic Communications and Transactions Act (25 of 2002)*.

4. CHAPTER 4: THE CLASSIFICATION OF ELECTRONIC EVIDENCE

4.1 Introduction

This chapter aims to provide an overview of how electronic evidence can be defined, as well as the different classification of evidence that can be considered as electronic evidence. Traditionally, the courts did not have much discretion regarding the admissibility of electronic evidence. The admissibility was limited to the same requirements that applied to documentary and hearsay evidence (Schwikkard & Van der Merwe, 2009:443). South Africa still has an "exclusionary approach to evidence" (Mason, 2007:459). The impact of this "exclusionary approach" to evidence is that courts tend to rather not allow evidence due to caution.

To understand the challenges that electronic evidence faces, it is critical to understand the traditional forms of evidence and where electronic evidence fits in. The three forms of evidence that will be discussed in this chapter are:

i. Documentary evidence;
ii. Real evidence; and
iii. Evidence as a product of an apparatus.

The *Electronic Communications and Transactions Act (25 of 2002)* also provides for the admissibility of data messages. Data messages as a form of evidence will therefore also be discussed in this chapter.

The *Computer Evidence Act 57 of 1983* (repealed) defined a computer as any device or apparatus, whether it is called a computer or not, that can interpret and calculate work performed by electronic, electromechanical, mechanical or any other means.

A computer will have the following characteristics (Mason, 2007:2):

i. It will receive information through any type of communication channel whether it is through a disk file or a keyboard*;*
ii. It will process the information entered or captured;
iii. It will produce an output of some sort whether it be on a computer disk or by means of a printer;
iv. It must be capable of storing information; and
v. It must be capable of controlling its workings.

Electronic documents can be considered as any format of a document other than the paper copy. It is also important to differentiate between the two ways in which electronic evidence may originate, namely:

i. Evidence from an analogue device, such as an audio tape and photographic films. Analogue devises create a form of data that is in a permanent form. Non-digital cameras will, for example, create a film with pictures taken and from the film the pictures can be developed. The film will be considered primary evidence, whereas the photos developed will be considered as secondary evidence.
ii. Digital evidence is anything that has been "created or stored on a computer or is made available by way of the Internet, including CDs, DVDs, and MP3" (Mason, 2007:21).

4.2 Documentary Evidence

4.2.1 Introduction

Documentary evidence plays an important role in South African law of evidence. A document can provide very strong evidence, since the wording is fixed and can be judged and re-judged by the court (Schmidt & Rademeyer, 1989:336). If a document is presented with the purpose of proving the content thereof, it would be considered to be documentary evidence. If a document is presented as an object, such as a counterfeit cheque, it would be considered as real evidence (Schutte, 2009:89).

The law of evidence requires that the best evidence available should be disclosed. For electronic evidence in the form of a computer printout, the best evidence would therefore be the original document (Timmer, 2011:57).

Section 33 of the *Civil Proceedings Act (25 of 1965)* states that the term *"document"* includes, but is not limited to, any book, drawing and photograph. Article 221 of the *Criminal Procedure Act (51 of 1977)* states that a document also includes any device through which information can be logged and stored. The *Criminal Procedure Act (51 of 1977)* therefore clearly allows for electronic evidence. A "device" can be considered any computer or other electronic medium. A computer is used to store data and process data. If the electronic evidence is therefore a result of storing information on a computer, such evidence may be considered as documentary evidence in terms of the *Criminal Procedure Act (51 of 1977)*.

In *R v Daye 1908 2 KB 333 340,* the judge defined a document as "any writing or printing capable of being made evidence". In the case of *Seccombe v Attorney-General 1919 TPD 270 277*, the judge commented that: "The word 'document' is a very wide term and includes everything that contains the written or pictorial proof of something".

In *S v Ndike & others (2006) JOL 18625 (Ck)*, the court concluded that a computer that is used for more than just storage, does not fall under the definition of a "document". In *S v Harper and Another 1981 (1) SA 88 (D)*, Milne J summarised the definition of a document as follows:

> If the computer printouts are documents that are within the ordinary grammatical meaning of that word, then they are admissible. If they are not, then, in my view they are inadmissible…Computers do record and store information but they do a great deal else; inter alia, they sort and collate information and make adjustments…The extended definition of 'document' is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than the mere storage or recording of information.

The aforementioned definition of a computer printout by Milne J is in line with the *Criminal Procedure Act (51 of 1977)*. If information was purely stored on the computer, such evidence would be considered documentary evidence and would be admissible if such evidence complies with the requirements of documentary evidence. If the computer performed any actions on evidence or made any alterations, then the computer was used for more than storing purposes and according to Milne J, such evidence would not be admissible.

In *S v Mpumlo and Others 1986 (3) SA 485 (E)*, Mullins J stated the following: that "a document in the form of writing or drawing or pictorial representation must be visible and capable of being read or interpreted by one's eyes".

Mullins J further stated that tape recordings and other audiovisual recordings are electronically recorded and the record is therefore not in writing. The judge did, however, add that documentary evidence must be in a form that a document normally takes, that is on paper or any similar material. The judge's definition of documentary evidence clearly exempts electronic evidence, such as video recordings, but if the judge's definition of "in writing" and "on paper" is applied then a computer printout could be considered as documentary evidence.

Once computer evidence has been ruled to meet the definition of documentary evidence, such evidence still needs to meet the requirements of admissibility of documentary evidence.

4.2.2 The admissibility of documentary evidence

In order for a document to be admissible in a court of law, the documentary evidence is subjective to three general rules:

i. The contents of the document can be proved by the production of the **original** document;
ii. Evidence is required to prove the **authenticity** of the document; and
iii. The document may have to be **stamped,** if so required by the *Stamp Duties Act 77 of 1968* (Zeffertt *et al.*, 2003:685).

The *Electronic Communications and Transactions Act (25 of 2002)* differentiates between "data" and "data message", which are defined as follows*:*

i. "Data message" means "data generated, sent, received or stored by electronic means and includes (a) voice, where the voices is used in an automated transaction; and (b) a stored record"; and
ii. "Data" means "electronic representations of information in any form".

Data messages are still vulnerable to errors and can be falsified in the same way as documents. "They cannot prove themselves to be anything other than data messages and their evidential value depends on witnesses who can both interpret them and establish their relevance. So as long as South African law follows an exclusionary approach it would seem that graphics, audio and video that are in data message form should be treated in the same way as documents" (Mason, 2007:473). As a result, not every data message will then be admissible. Data messages may be inadmissible due to grounds included in other legislation (Mason, 2007:463). Section 15(1)(b) of the *Electronic Communications and Transactions Act (25 of 2002)* further stipulates that data messages are admissible if in their original form, and data messages that are not in their original form would therefore be excluded (Mason, 2007:463).

Data messages that are found to be inadmissible in terms of the *Electronic Communications and Transactions Act (25 of 2002)*, but resemble documents can comply

with the rules of documentary evidence (Mason, 2007:464). Data messages treated as documentary evidence therefore should also comply with the following requirements:

i. Production;
ii. Original form; and
iii. Authenticity.

The aforementioned requirements of documentary evidence and data messages are discussed in more detail below.

Original form

The first requirement of documentary evidence is that the document should be in its original form (Bellengère *et al.,* 2013:74). Originality is also one of the challenges when dealing with electronic evidence, because a computer printout is not considered to be the original document. If the document was scanned into the computer the electronic version thereof would not be the original document. If the document was created on the computer, then the original would be on the computer hard drive and the computer printout would be the copy. Even then, the origins of the original document would be difficult to determine due to the fact that electronic documents can easily be altered.

The court will only accept secondary evidence of the document if the court is satisfied "that the original document in fact existed, that it has been lost or destroyed, and a reasonable explanation for its non-production has been given" (Timmer, 2011:58). The relevant rule of evidence is that "no evidence is ordinarily admissible to prove the contents of a document except the original document itself" (*Barclays Western Bank Ltd v Creser 1982 (2) SA 104 (T)*).

In *Barclays Western Bank v Creser 1982 (2) SA 104 (T)* the hard copies of documents were systematically being destroyed in a process of converting their system to an electronic storage system. When no original documentation was available, the court ruled that it was a "reasonable explanation" (Timmer, 2011:58).

The same requirements of documentary evidence are applicable to the originality of data messages. Section 14(1) of the *Electronic Communications and Transactions Act (25 of 2002)* states that if the law requires information to be in an original form, data messages will meet such requirement if the integrity of the data message was maintained and if the information is capable of being displayed or presented. Section 14(2)

determines how the integrity of data messages can be ascertained or assessed. The *Electronic Communications and Transactions Act (25 of 2002)* states that one should consider whether the information has remained intact and is therefore unaltered. Any changes that have been made to the information should have occurred in the normal course of collecting, storing and displaying of the evidence. The purpose for which the information was generated should be determined. Any other relevant factors should also be considered. Section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* also makes the provision that if the data message is the best evidence, it may be admissible even if such data message is not in its original form (Mason 2007:465).

The last exception of originality is provided for by the *Stamp Duties Act (77 of 1968)*. Section 12 states that

> No instrument which is required to be stamped under this Act shall be made available for any purpose whatever unless it is duly stamped, and in particular shall not be produced or given in evidence or be made available in any court of law.

This is, however, not applicable in criminal proceedings (Zeffertt *et al.*, 2003:699). Electronic evidence originates on a computer, and will therefore not be stamped. This general rule is therefore not applicable to computer evidence.

The challenges facing electronic evidence as a result of the original form requirement will be discussed in detail in Chapter 5 of this study.

Authenticity

The second requirement of documentary evidence is that the evidence must be proven to be authentic (Bellengère *et al.,* 2013:74). If a document can proved to be authentic, then the document may be considered to be reliable. To prove the authenticity of documentary evidence it is important to differentiate between private and public documents, as they are treated differently in court (Schmidt & Rademeyer, 1989:337).

A public document is any document by a public official in the execution of his/her duties, for a public service. The public should have access to public documents (Schmidt & Rademeyer, 1989:353). Private documents are any documents of an individual or a legal entity, which the public does not have access to. Most documents are considered to be private documents (Schmidt & Rademeyer, 1989:337).

The *Criminal Procedure Act (51 of 1977)* provides for the admissibility of public documents. Section 233 of the *Criminal Procedure Act (51 of 1977)* allows for copies of original documents to be admissible if the document "purports to be signed and certified as a true copy or extract by the officer to whose custody the original is entrusted."

The general rule for private documents is that the document must be presented in court as evidence by the author or by a witness that can prove the authenticity of the document. The document may be presented by the following (Schmidt & Rademeyer, 1989:339-341):

i. The author or the signatory: This individual will be in the best position to identify the document and to testify to the authenticity of the document;
ii. A witness: A witness that saw the document being signed or somebody that can by right identify and testify to the authenticity of the document;
iii. An individual that can identify handwriting: The authenticity of the document can be proved by means of a witness that can identify the handwriting or the signature of the person that created or signed the document, because he/she is either familiar with it or if he/she is a handwriting specialist. This means of evidence is only admissible if the author or a witness is not known;
iv. An individual that located the document in the opponent's possession or control: Documents that are located in an individual's possession or under his/her control are normally admissible against the individual. In such cases it is sufficient if the individual who located the document, identifies it; and
v. An individual under whose authorised supervision and control the document is: In some cases it is acceptable that a document may be presented by the individual under whose supervision and control the document is. In these cases there are two types of documents:
    - Documents older than 20 years: Legislation indicates that documents older than 20 years may be considered authentic if the document is located in the person's possession where one would expect to find it. The fact that the document is admissible does not mean that the content thereof is true; the hearsay rule is still applicable; and
    - Official documents: When an original official document is presented the author need not present it. An authorised individual may present the document. If it is a certified copy document may be presented.

There are some exceptions to the general rule. In the following instances the document need not be identified by a witness in order to prove the authenticity (Schmidt & Rademeyer, 1989:342):

i. When the document disclosed by the opponent and he/she is requested to disclose it before the hearing;
ii. When judicial notice is taken thereof;
iii. When the opponent acknowledges the authenticity of the document; and
iv. When the document is admissible through legislation by simply presenting the document.

Most documents are considered to be private documents and therefore most electronic evidence will also be considered as private documents.

The same requirements of authenticity that apply to documentary evidence is applicable to data messages, i.e. that the data message or document "is what it claims to be" (Mason, 2007:466).

Section 15(4) of the *Electronic Communications and Transactions Act (25 of 2002)* provides additional provisions for the authentication of data messages. The *Electronic Communications and Transactions Act (25 of 2002)* determines that if the data message was made by an individual in the normal course of business, a copy or computer printout of such data message can be certified and such evidence would be admissible on its mere production during any legal proceedings. The copy or computer printout has to be certified by an officer in service of the individual who made the statement.

As with documentary evidence, official documents and data messages do not need to be authenticated. Sections 18 and 19(3) of the *Electronic Communications and Transactions Act (25 of 2002)* make provision for "electronic notarisation, certification and sealing of data messages". The data message therefore has an electronic signature (Mason, 2007:466).

The requirement of authenticity of documentary evidence will be discussed in detail in Chapter 5 of this study.

Production

For a data message to be admissible, it must be produced, but because it is not possible for humans to detect the electronic signals contained in a data message, a computer or other electronic media would be necessary to display the data message (Mason, 2007:464).

Section 17 of the *Electronic Communications and Transactions Act (25 of 2002)* addresses the production requirement of data messages. Section 17(1) determines that if a person is required by law to produce a document or any other information, such requirement is met, if the individual produces a computer printout or document, by means of a data message. Certain requirements, however apply, namely:

i. All circumstances at the time the message was sent should be considered. The method whereby the information was generated provides a valuable means by which the integrity can be ascertained and maintained; and
ii. It is reasonable to expect that at the time the information was sent, it would be readily computable and in a form to be used for later reference.

Section 17 of the *Electronic Communications and Transactions Act (25 of 2002)* therefore allows for an individual who is legally required to produce the document in the form of a data message to do so, if the requirements of integrity are met (Mason, 2007:464).

4.3 Real Evidence

Real evidence is evidence that is disclosed to the court in the form of an object. Real evidence includes videos and graphics (Mason, 2007:472). If a document is submitted to prove the contents thereof, such documents would be considered to be documentary evidence. If the document is, however, submitted purely as an object, such evidence would be considered to be real evidence (Schmidt & Rademeyer, 1989:326)

Real evidence differs from documentary evidence in that real evidence is always admissible if it is relevant and meaningful (Schmidt & Rademeyer 1989:326).

In *S v Mpumlo [1986] 4 All197 (E)*, the state argued that a videotape is real evidence and therefore not subject to the requirements of documentary evidence. The accused argued that no statutory or any other authority allowed for video tapes to be admissible. Alternatively, the accused argued that the video tape was nothing more than a “series of

images" and would therefore have to comply with the requirements of documentary evidence. Mullins J made the following judgment:

> I have no doubt that a video film, like a tape recording, is real evidence, as distinct from documentary evidence, and, provided it is relevant, it may be produced as admissible evidence, subject of course to any dispute that may arise either as to its authenticity or the interpretation thereof.

In *S v Smuts 1972 4 (SA) 358 (T)*, the court ruled that if a computer is used as a speed trap, the reading of the computer would be considered as real evidence and not hearsay evidence, because the computer created the reading without any human input.

In England, the case of *The Statue of Liberty [1968] 2 All ER 195*, radar soundings of a ship's movements were admissible as real evidence and not hearsay evidence, because the machine was operating without any human input.

If a computer program is used in equipment and the equipment can produce data without any human intervention, then the data will be considered to be real evidence (Mason, 2007:473). If the evidence was, however, created in part from human input, the hearsay rules would apply, and only if concluded that it is not hearsay would the evidence be admissible (Zeffertt *et al.*, 2003:712).

4.4 Evidence as the product of an apparatus

Traditionally there are three categories of evidence, namely *viva voce* evidence, which is evidence that is delivered orally, documentary evidence and real evidence. Evidence as the product of an apparatus is usually divided into documentary evidence and real evidence (Schutte 2009:104). A computer is a perfect example of an apparatus from which evidence may derive.

Like documentary evidence, evidence as a product on an apparatus, should also be disclosed and the authenticity thereof should be proven. When disclosing the type of apparatus used, it is important to prove that it is reliable. It should therefore be verified that the computer is a reliable instrument for the purpose for which it is being used (Schutte, 2009:104).

In a considerable number of cases the reliability of the individual working with the computer should also be verified (Schutte, 2009:104). De Villiers J commented in *S v Mutle 1970 4 SA 535 (T) 537* that it is an acceptable practice, that if the state is relying on the evidence from an apparatus, it should be verified by an expert witness. The court

further stated that the expert witness should testify that the apparatus is a reliable instrument and that when the evidence was created, it was functioning accurately.

In the cases of *S v Pennels 1977 1 SA 809 (N)* and *S v Claassen 1976 2 SA 281 (O)*, it was concluded that if there is any doubt regarding the reliability of the evidence created by the apparatus, the court may not conclude any findings on this evidence.

The requirement of reliability will be discussed in further detail in Chapter 5 of this study.

4.5 Conclusion

Electronic evidence can be either documentary evidence, real evidence or evidence as the product of an apparatus. Each form of evidence has its own set of rules and admissibility requirements that should be met. Each form of evidence furthermore has its own set of challenges. The challenges that electronic evidence faces are discussed in Chapter 5 of this study.

5. CHAPTER 5: CHALLANGES FACING ELECTRONIC EVIDENCE

5.1 Introduction

Even though law enforcement is aware of economic crimes, it has been found to lack the knowledge and training to successfully deal with economic crimes (Manning, 2005:v*).*

Detailed procedures for gathering and storing electronic evidence in order for the South African law to be fully applicable and effective are lacking in South Africa (Mason, 2005:485). In the Mashiyi case the court stated the following regarding electronic evidence "that these lacunae in our law be filled and for new legislation relating specifically to electronic evidence in criminal cases be considered" (*S v Mashiyi 2002 (2) SASV 387 (Tk)*):

Electronic evidence is *"*undeniably problematic". The moment technology moved away from pen and paper, most guarantees of reliability and authenticity were left behind (Mason, 2007:459).

As discussed in Chapter 4, electronic evidence can be classified as the following evidence:

i. Documentary evidence;
ii. Real evidence; and
iii. Evidence as a product of an apparatus.

The first issue electronic evidence faces is simply what type of evidence it is. After the electronic or electronic evidence has been correctly classified, it comes up against the unique set of laws and accompanying challenges that each type of evidence faces.

From Chapter 4 it is evident that the general challenges that electronic evidence is faced with are as follows:

iv. Hearsay evidence;
v. Originality;
vi. Authenticity; and
vii. Reliability.

These general challenges relating to electronic evidence will be discussed below.

5.2 Hearsay evidence

When determining what type of evidence electronic evidence is, the first and most important step is to determine for what purpose the computer or electronic apparatus was used. Was the computer used to simply store information? Was the information on the computer captured by an individual or did the computer process information without or with human input?

In the case of *S v Mashiyi & another (2002) JOL 9894* two types of electronic evidence were present:

i. Computer printouts of documents that were simply stored on the computer. These printouts were judged to be admissible; and
ii. Computer printouts of information that was processed by the computer. These printouts were considered to be hearsay evidence.

When evidence is submitted simply to prove a fact, it will not be excluded by the South African law. When evidence is, however, submitted to show the truth of its contents, the South African law requires that the individual presenting the evidence be cross-examined. If cross examination cannot be executed, the evidence will be considered hearsay evidence and will be inadmissible, unless it complies with the exceptions of the hearsay rules (Mason, 2007:466).

5.2.1 Definition of hearsay evidence

"If Y is charged with murdering Z, and a witness, W, testifies that a friend of his, X, told him that he saw Y shoot Z on the day in question, should this evidence be received?" (Zeffertt *et al.*, 2003:361). Hearsay evidence is therefore evidence of that which another person told the witness. The witness merely relays what he or she heard (Schmidt & Rademeyer, 1989:472). Watermeyer J provided the following definition of hearsay evidence in the case of *Estate De Wet v De Wet 1924 CPD 341:* "evidence of statements made by persons not called as witnesses who are tendered to prove the truth of what is contained in the statement."

Hearsay evidence is evidence of that which another person told the witness. The witness merely relays what he or she heard (Schmidt & Rademeyer, 1989:472). Hearsay evidence is inadmissible, because it is normally unreliable and for that reason can mislead the court. It is unreliable since the individual who observed the facts, does not testify and

inform the court of his/her observations in person. Furthermore, the individual who observed the facts is not subject to the oath of the court. His or her testimony can also not be questioned under cross-examination (Schmidt & Rademeyer, 1989:472-473).

In terms of section 3(4) of the *Law of Evidence Amendment Act (45 of 1988)*, hearsay evidence can be defined as evidence, oral or in writing, where the probative value of the evidence "depends on the credibility of any person" not providing the evidence.

In terms of electronic evidence, hearsay evidence is therefore information that was captured by an individual on a computer and the computer stored or processed the information. Human error is therefore prevalent and for this reason such documents would be considered as unreliable.

5.2.2 Rules of hearsay evidence

In order for hearsay evidence to be admissible, the evidence must comply with certain rules.

Section 3(1) of the *Law of Evidence Amendment Act (45 of 1988)* stipulates that, subject to other laws, hearsay evidence will not be allowed as evidence during legal proceedings unless the party, against whom the evidence is submitted, agrees to such evidence and if the individual upon "whose credibility the probative value of such evidence depends" testifies during the legal proceedings. Section 3(2) of the *Law of Evidence Amendment Act (45 of 1988)* states that evidence that is inadmissible on any other ground other that hearsay, will not be made admissible due to the provisions of section 3(1) of the *Law of Evidence Amendment Act (45 of 1988).*

Section 3(3) of the *Law of Evidence Amendment Act (45 of 1988)* states that hearsay may be provisionally allowed if the court has been informed that the individual upon "whose credibility the probative value of such evidence depends" will testify during the proceedings. If that individual does not later testify during the proceedings, such evidence will left out.

Van Zyl J made the following remark in respect of section 3 of the *Law of Evidence Amendment Act (45 of 1988)* in *S v Ndike 2008 (2) SASV 252:*

> If a computer printout contains a statement of which a person has personal knowledge and which is stored in the computer's memory, its use in evidence depends on the credibility of an identifiable person and would therefore constitute hearsay. On the other hand, where the probative value

of a statement in the print-out is dependent upon the 'credibility' of the computer itself, section 3 will not apply.

Section 34(1) of the *Civil Proceedings Evidence Act (25 of 1965)* should be read in conjunction with section 3 of the *Law of Evidence Amendment Act (45 of 1988).* The *Civil Proceedings Evidence Act (25 of 1965)* states that during any civil proceedings where *viva voce* evidence would be admissible, any statement made by that person in the form of a document, will be admissible provided that the original be produced. The person who made the statement, however, either had to have personal knowledge of the facts contained in the document or, if the document forms part of a continuous record that was made in performing his/her duty, to record information provided to him/her by an individual who had personal knowledge of the facts contained in the document.

South African law requires the individual who made the statement to testify during the court proceedings. Section 34(1)(b) of the *Civil Proceedings Evidence Act (25 of 1965)* includes various exclusions to that rule. The individual who made the statement will be excused if such individual:

i. Is dead;
ii. Is unfit due to a bodily or mental condition;
iii. Is outside the Republic of South Africa and it is not reasonably possible to secure his/her attendance at the proceedings; or
iv. All reasonable efforts have been made to secure the individual's attendance without success.

5.2.3 The admissibility of hearsay evidence

Electronic evidence regarded as hearsay evidence is therefore admissible if the individual against whom the evidence is submitted, agrees to the admission of the electronic evidence (Schmidt & Rademeyer, 1989:476). Electronic evidence will also be admitted if the individual, who captured the information on the computer, can testify that he or she did capture the information and that the information was captured accurately. However, the challenge that arises is that computer evidence, in most instances, is not only captured by one individual. If the computer evidence was therefore captured by various, independent individuals, they may or may not know if the information they captured was correct and accurate (Schutte, 2009:111).

Section 3(c) of the *Law of Evidence Amendment Act (45 of 1988)* stipulates that the court may decide to admit hearsay evidence if the court is of the opinion that the hearsay evidence may be in the interest of justice. The court will consider the following factors:

i. The nature of the proceedings and the evidence;
ii. Why the evidence is admitted;
iii. The probative value of the hearsay evidence;
iv. Why the evidence is not provided by the person upon whose credibly the probative value of the evidence depends;
v. If any party can be disadvantaged by admitting the hearsay evidence; and
vi. Any other factor in the opinion of the court that should be taken into account.

According to section 3(c) of the *Law of Evidence Amendment Act (45 of 1988)*, the probative value of the evidence also impacts the court's decision on whether the hearsay evidence should be admissible. The court needs to establish what conclusions can be drawn based on the hearsay evidence. If the credibility of the evidence depends on an individual who cannot be identified, the court has to determine what value can be added to the points in dispute. In *S v Ramavhale 1996 1 SASV 639 (A)*, the court found that the hearsay evidence applicable could not be admitted for the following reasons:

i. The probative value of the hearsay evidence was minimal; and
ii. The hearsay evidence had the potential to disadvantage the accused.

Section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* states that law of evidence should not deny the admissibility of data messages on the mere grounds that it is a data message. If further states that if the evidence is the best evidence that could or could reasonably be expected to be obtained, the evidence should not be denied on the grounds that it is not in its original form.

In *Ndlovu v Minister of Correctional Services & Another 2004 JDR 0328 (W)* the admissibility of a computer printout was in dispute. The computer printout was in the form of a diary, reflecting the monitoring of the parolee from his release until date of printout. The entries into the diary were made by the parole officer or a monitor. Ndlovu argued that the computer printout was not the original, as it was a computer printout and the court should not allow it unless properly proved. The court analysed whether the printout should be admissible or not in terms of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* read in conjunction with section 3 of the *Law of Evidence*

Amendment Act (45 of 1988). The court found the printout admissible, not because of the provisions of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)*, but rather in terms of the exclusion rules to hearsay in section 3 of the *Law of Evidence Amendment Act (45 of 1988)*, which allow the court's discretion to allow hearsay evidence.

As indicated in Chapter 3 of this study, it is unclear whether the purpose of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* is to allow all hearsay evidence to be admissible.

Hearsay has been recognised as a major hurdle when dealing with electronic evidence. The South African Law Reform Commission issued Paper 27 on the admissibility of electronic evidence. The Commission was specifically concerned with the relationship between the *Electronic Communications and Transactions Act (25 of 2002)* and the hearsay rule. The SALRC has, however, not published the report on this project as yet. The findings of this project will be significant and may shape future legislation dealing with electronic evidence.

5.3 Originality

Electronic evidence in the form of a computer print-out will, in the most instances, have to comply with the requirements of documentary evidence. One of the requirements of documentary evidence to be admissible is that the original document has to be presented. This rule is known as the best evidence rule (Schutte, 2009:97).

When the content of the document is not in dispute and the document is therefore not submitted to prove its contents, an original document is not required (Zeffertt *et al.*, 2003:688).

When the content of the document is formally admitted, the original document need not be submitted. The normal rules of admission will, however, still apply (Schmidt & Rademeyer, 1989:347).

In some instances a party may adduce secondary evidence to prove the contents of a document. The general rule is that the production of the original document is excused; the document may be proved by copies thereof or by oral evidence of an individual that can recall the document's contents (Zeffertt *et al.*, 2003:690).

Secondary evidence may be submitted in the following instances:

i. If the document is in the possession of the opposition: When the original document is in the possession of the opposing party and he or she has failed to produce the document after a reasonable amount of time, secondary evidence may be submitted;
ii. If the document is in the possession of a third party: If the original document is in the possession of a third party, the correct procedure would be to serve him or her with a subpoena requesting the original document. Secondary evidence may, however, be accepted if the third party can legally refuse to do so in terms of privilege or if the evidence will be inadmissible due to the third party residing outside the jurisdiction of the proceedings. An effort, however, has to be made to obtain the original document from the third party;
iii. If the original document has been destroyed or is lost: Secondary evidence may be submitted if it can be shown that the document is lost after a proper search to locate the original document (Zeffertt *et al.,* 2004:690-694). In *Barclays Western Bank v Creser 1982 (2) SA 104 (T)* original documentation was systematically being destroyed in the process of converting their storage systems to an electronic storage system. The court held that this was a reasonable explanation for non-production of the original documents.
iv. If the production of the original document is impossible or inconvenient: In *Watts and Darlow v R 1919 NPD* it was found to produce a tombstone with writing on would be impossible or inconvenient to produce;
v. If the original document is a public document;
vi. If the original document is an official document; and
vii. Other statutory exemptions (Zeffertt *et al.,* 2003:690-694).

The challenge that arises in respect of electronic evidence is that the computer print-out will never be the original document. The computer print-out is therefore not the original, but also not a duplicate of the original. A further challenge that computer print-outs create is that large quantities of documents are compiled from other documents, and not all documents will be known (Schutte, 2009:110).

5.4 Authenticity

The general rule is that the party who tenders documentary evidence also has to adduce evidence to prove to the court that the document is authentic. Normally, the author of the document therefore has to testify that he or she did write or execute the document (Zeffertt *et al.,* 2003:694).

If the authenticity of a document cannot be established, not only will it be inadmissible but it also cannot be used for purposes of cross-examination. It is, however, possible that the document be provisionally allowed and that it can be used for the purpose of cross-examination. The decision regarding the authenticity of the document will then be postponed to the end of the proceedings (Schmidt & Rademeyer, 1989:339).

The following parties can testify regarding the authenticity of a document:

i. The author or the signatory of the document as this party will be the best possible witness to identify the document and to prove its authenticity;
ii. A witness who can testify that he or she witnessed the author create the document or who witnesses the document being signed;
iii. A party who can identify the handwriting on the document, either because he or she is known with the handwriting of the author or the signatory, or if the party is a handwriting specialist. Evidence in this form will only be accepted if the author or the signatory is not available;
iv. A party who located the document in the opposing party's possession or under the opposing party's control. In such instances if is sufficient if the individual who located the document testifies that he or she did so; and
v. A party under whose legitimate control and care the document is. Two specific types of document are prevalent in such instances, namely documents that are older than 20 years and official documents (Schmidt & Rademeyer, 1989:340-341).

Certain types of document are, however, admissible upon production thereof, without proof of their authenticity (Zeffertt *et al.*, 2003:696). These exceptions to the general rule are:

i. Public documents: Based on Section 233 of the *Criminal Procedure Act (51 of 1977)*, public documents allow for copies of public documents and such

copies shall be admissible if signed and certified as a true copy by the individual under whose legitimate control or custody the original is;

ii. In most instances certified copies that are deemed admissible, also need to prove the authenticity thereof (Zeffertt *et al.,* 2003:697). Section 246 of the *Criminal Procedure Act (51 of 1977)* makes provision for documents that have been signed by an individual holding public office and have been stamped or sealed by the relevant department, office or institution. In *S v Kekane and others 1986 (4) SA 466 (T)* it was said that an example of such a document was permitted;

iii. Ancient documents: Section 37 of the *Civil Proceedings Act (25 of 1965)* and applied in section 222 of the *Criminal Procedure Act (51 of 1977)* states that documents that are older than 20 years are considered to be ancient documents. Ancient documents that come from "proper custody are presumed to have been duly executed if there is nothing to suggest the contrary" are admissible (Zeffertt *et al.*, 2003:698). This exception would not be as prevalent for electronic evidence;

iv. Foreign documents: Based on Supreme Court Rule 63, documents executed abroad, are admissible if the documents have been authenticated in terms of the Supreme Court Rule 63 (Zeffertt *et al.*, 2003:698-699). In *Chopra v Sparks Cinemas (Pty) ltd and Another 1973 (2) SA 352 (D)*, Henning J held that this rule is, however, not absolute.

The proof of authenticity creates various issues for electronic evidence. In many instances the author will be unknown or a document will have various authors. If the author can be identified, the documents authenticity is still in question for the following reasons:

i. The author merely captured the information with which he/she was provided;
ii. The information provided could have been incorrect;
iii. The author could have captured the information incorrectly; and
iv. Electronic evidence is easily altered or deleted.

The possibility of falsifying or forging electronic information is just too great.

It was held in *Knouwds v Administrateur, Kaap 1981 1 SA 544 (K)* that even if a document is proven to be authentic it is not necessarily admissible. The document still has to comply with the normal rules of admissibility. The document must therefore not be irrelevant, hearsay evidence (Schutte, 2009:99).

5.5 Reliability

When electronic evidence is deemed evidence as the product of an apparatus, it has to be proven that the computer used was reliable; in other words, that the computer functioned normally and that its operator used it correctly (Schmidt & Rademeyer; 1989:359).

The proof of reliability also stems from the proof of relevancy, since only a product from a reliable apparatus can provide evidence from which a reasonable conclusion can be drawn (Schmidt & Rademeyer, 1989:359). The United States of America's *Federal Rules of Evidence*, Rule 401, defines relevant evidence as "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence".

Proof of reliability is normally provided by an expert witness. In *S v Margolis 1964 4 SA 579 (T) 582*, the court required evidence of the reliability of a speedometer. Evidence to prove the speedometer's workings over a period of months, as well as proof of services was required. In some instances, judicial notice can be taken of evidence if there is a presumption of normal functionality (*Fischer v R 1938 2 PH 044 (O)*). The evidence, however, depends on the nature and the familiarity of the apparatus, as well as the purpose for which the apparatus is used (Schmidt & Rademeyer, 1989:359-360).

It is not always solely the reliability of the computer itself that is in question. The reliability of the operator of the computer may also be in dispute. In *S v Bornman 1975 1 SA 658 (T)*, a traffic officer followed the vehicle of the accused for six kilometres. The traffic officer's vehicle's speedometer indicated that the vehicle in question travelled at 140 kilometres per hour. The traffic officer's speedometer was tested and found in order. The court was, however, not prepared to rule that the accused travelled at a speed of more than 80 kilometres per hour.

When considering the nature of the evidence, one has to consider the reliability of the evidence. The general rule of hearsay evidence is that it is inadmissible due to the fact that it is unreliable and has the potential to mislead the court. Electronic evidence is by nature unreliable and the reasons may include:

i. The individual operating the computer or creating the document may be unknown;
ii. The individual capturing the information could have captured the information incorrectly, either accidently or on purpose; and
iii. Information stored on a computer can easily be altered or deleted (Schutte, 2009:111).

5.6 Conclusion

As is evident from the above, the challenges that electronic evidence faces are vast. Very few of the challenges are fully addressed by legislation. The issue of originality is mostly addressed by legislation. The issues of hearsay, authenticity and reliability, however, are only partly dealt with by legislation. Clarity should be obtained concerning the purpose of the *Electronic Communications and Transactions Act (25 of 2002)* with regard to the aforementioned issues.

6. CHAPTER 6: THE COLLECTION AND STORAGE OF ELECTRONIC EVIDENCE

6.1 Introduction

Digital forensic science can be defined as the investigation of data or information stored on all devices that can contain electronic information, for example computers and cell phones. It furthermore includes the recovery of such information stored on the device for prosecution purposes, whether for civil or criminal proceedings (Bellengère *et al*., 2003:354).

The role of the forensic practitioner is critical, even before the evidence is presented in a court of law. To ensure that electronic evidence will be admissible in a court, the evidence has to be obtained in the best or most acceptable manner.

This chapter aims to address methods on how to gather, store and present computer-generated evidence.

6.2 Investigation of a crime

The investigation of a crime can be defined as a "systematic, organized search for the truth". An investigation furthermore entails the gathering of evidence, whether objective or subjective, relating to certain allegations or incidents (Van Rooyen, 2004:6).

An investigation can be divided into three phases. These phases are as follows:

i. Preliminary phase. During this phase the forensic practitioner will gather the evidence at the crime scene or other locations of interest (Van Rooyen, 2004:18). During this phase the forensic practitioner will identify the relevant evidence whether it is in the form of a computer printout, a hard drive of a computer, cell phones, etcetera. The type of storage device may determine the manner in which the information is dealt with;
ii. Follow-up investigation. During this phase the forensic practitioner performs follow-up consultations and requests further documents to corroborate preliminary findings. This phase includes obtaining subject matter experts, such as computer experts (Van Rooyen, 2004:18). Not all forensic practitioners will be experts in computer analyses. It may therefore be imperative to obtain the expertise of experts to ensure that evidence is gathered and analysed in the best manner.

Most of the bigger forensic firms have their own forensic technology teams who assist the investigations teams in gathering and analysing electronic evidence; and

iii. Trial phase. During this phase the relationship between the forensic accountant and the police is critical. The evidence in itself is only one part of the process of court proceedings. The forensic accountant will furthermore assist in the following functions (Van Rooyen, 2004:18):
   - to ensure that witness statements have been taken down;
   - to ensure that the evidence is available to the court; and
   - to ensure that the exhibits of the findings be presented in the court.

When performing an investigation, the forensic practitioner needs to be aware at all times of the admissibility of evidence. All information that is collected during the investigation must at least pass the three principle tests of admissibility. The three tests are (Van Rooyen, 2004:17):

i. Relevance;
ii. Materiality; and
iii. Competency.

6.3 Gathering and analysing

During evidence recovery it is critical to have expert forensic practitioners to recover the information. If an expert forensic practitioner is not utilised, the integrity of data will in most cases be compromised and therefore the evidence will be inadmissible in a court of law (Van Rooyen, 2004:175).

Since there is no standardised approach to gathering and storing electronic evidence, it is useful to consider the different approaches authors and industry leaders have to this process.

Van Rooyen's approach on how to recover evidence in order to address the legal challenges such evidence faces in court is as follows:

i. **The collection phase:** During this phase electronic evidence is identified, collected and documented. This phase is critical to ensure that no information gets compromised or lost;

ii. **The examination process:** During this phase the forensic practitioner will discover what is enclosed in the evidence. The state of the evidence is also determined; and

iii. **The analysis phase**: When seizing the electronic evidence, the forensic accountant should maintain its integrity. The electronic evidence has to be presented to the court in a form that the court will understand. It is therefore of the utmost importance to prove that the evidence has not been influenced or fabricated. During this phase, the forensic practitioner should take detailed notes on how the evidence is recovered. During litigation, the forensic practitioner may be questioned on the processes he/she followed to secure the evidence.

A recent study has highlighted the follow key aspects of the investigation process (Hershensohn, 2005:10-14):

i. **Authorisation:** It should be determined if the individual collecting the electronic evidence is duly authorised to do so. A search warrant is an example of a duly authorised collection of evidence;

ii. **Acquisition:** When the computer evidence is collected, it should be done in a manner that maintains the evidence in its original form;

iv. **Authentication:** The investigator collecting the data should ensure that the electronic evidence is authentic and in its original form. As authentication is a requirement for evidence to admitted, the investigator should bear that in mind when performing the analysis on the information;

v. **Analysis:** The information contained in the electronic evidence should be analysed, free from bias. It should be possible that the results of the analyses be verified by a third party;

vi. **Reporting:** The investigator should present his/her findings in a reasoned manner, along with the actions performed by the investigator to come to such findings; and

vii. **Testimony:** The investigator should be able to present his/her findings and to testify about such findings in a court of law.

The Association of Chief Police Officers (APCO, 2011) states that when recovering computer-generated evidence, the stages of recovery will *inter alia* be the following:

i. The collection phase: This phase entails identifying the sources of electronic evidence, searching for such evidence, collecting the evidence and documenting the process;

ii. The examination phase: During this phase the significance and the origin of the electronic evidence is determined. The investigator should record the state, as well as the content of the electronic evidence in its entirety. This allows the investigator to determine what is contained in the electronic evidence and in doing so to identify any information hidden in the evidence;
iii. The analysing phase: During this phase the investigator reviews the results of the examination phase along with determining the probative value and the significance of the electronic evidence; and
iv. The reporting phase: During this phase the examination process is outlined. The steps taken during the abovementioned phases need to be fully documented in order for the investigator to testify in a court of law.

APCO (2011) further highlights the following four principles when dealing with electronic evidence:

i. No action should be taken by the investigator to change any of the information contained in the electronic evidence if such evidence may be relied on in a court of law;
ii. Under circumstances where the information contained in the electronic evidence should be accessed, the investigator doing such should be experienced and capable of doing so. The investigator would then also be expected to provide evidence relating to why such actions were relevant and what the impact of such actions was.
iii. All steps taken during the collection, storage and analysis of the electronic evidence should be clearly documented and properly kept. A third party should be in a position to re-examine the information and should come to the same conclusion; and
iv. The investigator in charge is responsible for ensuring that all laws and principles are abided by.

The 13th INTERPOL Forensic Science Symposium, held in France during 2011, established the following principles when collecting electronic evidence (Interpol, 2011):

i. When the investigator collects the electronic evidence, care should be taken not to compromise and change the evidence;
ii. The investigator accessing the information within the electronic evidence must be trained or competent to do so;

iii. Every step taken during the collection, storage and analysis phase must be clearly documented in order to be reviewed;
iv. If the electronic evidence is in the possession of the investigator, that investigator is responsible for all steps taken relating to such evidence; and
v. If another agency is utilised to perform the search and seizure, gathering the evidence or to store the evidence, that agency should also comply with the aforementioned principles.

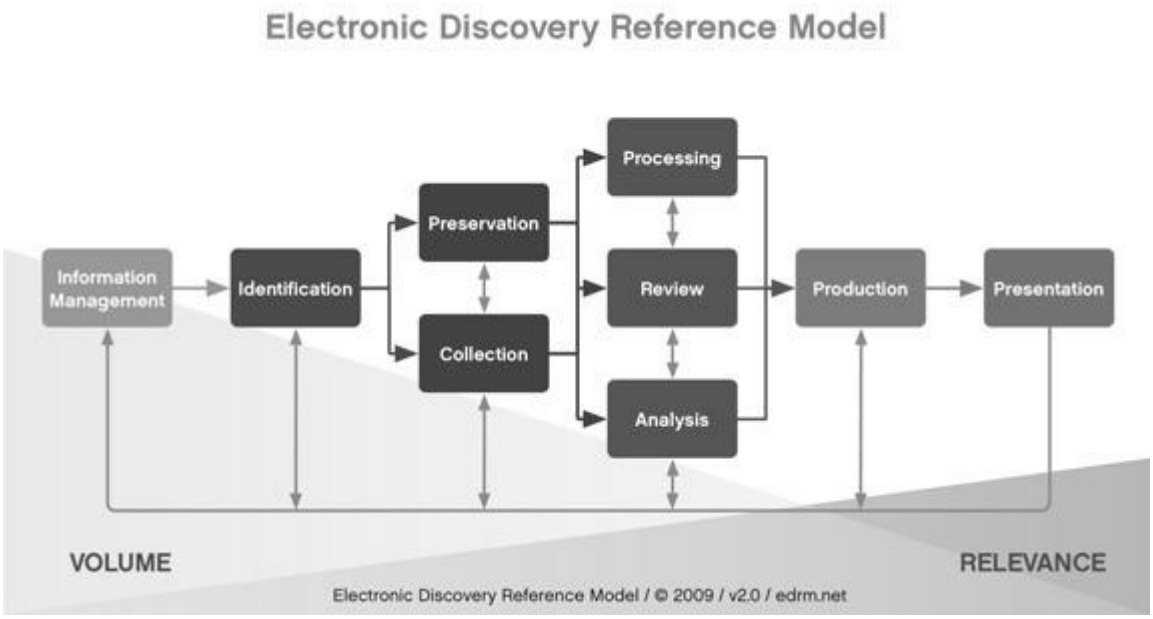
As a summary of the aforementioned, the following similarities can be drawn, which will reflect an ideal structure of how electronic evidence should be gathered and analysed:

i. **Collection phase:** The location and the various forms of electronic media should be determined in advance in order to specify what information is required. The forensic investigator collecting the electronic evidence should be duly authorised to do so. Care should be taken to ensure that the integrity of the evidence stays intact;
ii. **Preserving and authentication phase:** The integrity, the origins and then authenticity of the electronic evidence should be determined. The forensic accountant should furthermore ensure that the information cannot be altered or modified;
iii. **The analysing or examination phase:** The electronic evidence should be analysed by the forensic accountant. The forensic accountant should document all the steps performed on the data as well as the methods that were applied. An unbiased third party should be able to come to the same conclusion as the forensic accountant; and
iv. **Presenting:** The forensic accountant should be able to present the evidence as well as the findings to a court of law. The evidence should therefore be in a presentable format. The forensic accountant should also be able to testify during legal proceedings.

6.4 The Electronic Discovery Reference Model (EDRM)

The electronic discovery reference model was published by the EDRM in January 2006. The EDRM comprises 260 organisations. The EDRM provides organisations with frameworks and standards on how to address electronic discovery.

Figure 2



Source: http://www.edrm.net/resources/guides/edrm-framework-guides

The EDRM, as illustrated above, includes the following steps when collecting, storing and presenting computer-based evidence:

i. **Identification:** During this phase, the electronic evidence is identified and its whereabouts determined;

ii. **Preservation:** During this phase, the investigator should ensure that the information cannot be altered or destroyed;

iii. **Collection:** During this phase, the electronic evidence is collected;

iv. **Processing:** During this phase, it may be necessary to reduce the volume of the information contained in the electronic evidence and to convert it into a more readable format;

v. **Review:** During this phase, the electronic evidence is reviewed to determine its relevancy to the investigation;

vi. **Analysis:** During this phase, the evidence is evaluated to determine the content thereof, as well as to add context;

vii. **Production:** During this phase, the findings of the examination process are presented to the relevant individuals in an appropriate form and method; and

viii. **Presentation:** During this phase, the findings are presented to an audience whether during a deposition or during a court trial.

Various forensic investigation practices, such as KPMG and Ernest & Young in South Africa prescribe to the EDRM (KPMG, 2013 & EY, 2010).

KPMG's Electronic Evidence and Discovery Services provide organisations with processes and technologies to address needs that may arise from investigations and litigation. Their services include the following (KPMG, 2013):

i. "Electronic data processing;

ii. Discovery management;

iii. Hosting for review and production; and

iv. Collection and analysis".

During the data collection phase, KPMG uses customised equipment to search, to collect and to analyse electronic evidence. The forensic practitioners are training to collect evidence in such a manner to be suitable for legal proceedings (KPMG, 2013).

According to Ernest & Young, electronic evidence that is properly prepared and disclosed can strengthen a party's position during litigation. The opposite is, however, also true (EY, 2010). Ernest & Young also refers to the electronic discovery reference model and therefore obtains computer-generated evidence while maintaining the integrity thereof.

6.5 Preserving electronic evidence

When dealing with any form of physical evidence, a proper chain of custody plays a pivotal role in ensuring the integrity of such evidence. Chain of custody can be described as the "continuous safekeeping and identification of physical evidence" (Van Rooyen; 2004:12). Chain of custody can also be described as a term "that is applied to consecutive custodians of the physical items or documents in their original condition".

The court must therefore be satisfied that the evidence is in the same condition as it was at the time of the crime (Manning, 2005:74)

It is therefore important that evidence is gathered and stored in a competent and expert manner in order for such evidence to be valuable during court proceedings. This necessitates the involvement of the forensic accountant, as well as ensuring that the right procedures are followed to ensure the chain of custody (Schwikkard & Van der Merwe, 2009:450).

6.6 Search and seizure legislation

In South Africa various pieces of legislation provide guidelines with regard to the search and seizure of electronic evidence. Chapter 2 of the *Criminal Procedure Act (51 of 1977)* provides guidelines for search warrants, search and seizures, as well as other methods of entering premises and obtaining information (Basdeo, 2012:204).

Section 20 of the *Criminal Procedure Act (51 of 1977)* determines that the State may seize anything, which on reasonable grounds:

i. is concerned with a crime or a suspected crime;
ii. may afford evidence in a crime or a suspected crime; or
iii. is intended to be used or believed to be used in a crime or a suspected crime.

Section 21 of the *Criminal Procedure Act (51 of 1977)* determines that an article may only be seized by means of a search warrant, which may be issued by a magistrate of justice, a judge or a judicial officer. A search warrant that has been issued requires a police official to seize the articles listed, to search the individuals listed and/or search the listed premises. Section 21(2) of the *Criminal Procedure Act (51 of 1977)* reads as follows: “a search warrant issued under ss(1) shall require a police official to seize the article in question and shall to that end authorize such police official to search”.

Sections 82 and 83 of the *Electronic Communications and Transactions Act (25 of 2002)* provide statutory bodies and cyber investigators certain powers of search and seizure. Section 82(2) of the *Electronic Communications and Transactions Act (25 of 2002)* states that any statutory body with the powers of search and seizure, may appoint a cyber-inspector to assist in an investigation, provided that that the statutory body apply to the Department of Communications in the prescribed manner and the Department of Communications approves such a request. Section 81 of the *Electronic Communications*

and Transactions Act (25 of 2002) stipulates that the Director General may appoint an employee of the Department of Communications as a cyber inspector.

No act in South Africa, however, specifically addresses the preservation and partial disclosure of computer-generated evidence and the traditional rules and regulations of search and seizure would apply (Basdeo, 2012:204).

As the South African Police Service has the authority to search and seize, they also have the power to appoint forensic accountants from the business sector (Mason, 2007:484). The problem is that companies initiate their own investigations and only after they have investigated the crime or losses, the complete investigation is handed to the police (Van Rooyen, 2004:3). In other words, they perform the investigation without a mandate to investigate from the police.

Motata J referred to article 21(2) of the *Criminal Procedure Act (51 of 1977)* in the judgment of *Extra Dimension and others v Kruger NO and others 2004 (2) SACR 493 (T).* The search warrant gave powers of search and seizure to police officers, as well as private individuals. The court held that the search warrant was invalid as it granted the private individuals "irregular" powers. The court concluded that it is clear that only police officers can be authorized to search and not private persons, even if they are named in the search warrant.

Another challenge regarding the gathering of electronic evidence is the items listed on the search warrants. Warrants should specify the items that can be seized and they can only seize items that are relevant to the case. In *Beheersmaatschappij Helling I NV and others v Magistrate, Cape Town, and Others 2007 (1) SACR 99 (C)* the police seized all the computers and central processing units of computers, hard drives and computer discs. They also imaged a computer hard drive on the scene. Not all the information on the computers, hard drives and other computer media was relevant to the case. The court stated that a search warrant should be drafted with reasonable strictness. As unrelated information was also seized, the court ruled that the warrants were therefore unlawful and invalid.

6.7 Conclusion

The need for standard procedures for gathering and storing electronic evidence in South Africa can be summarised perfectly as follows (Mason, 2007:485):

> What is missing in the South African law of electronic evidence are detailed procedures that the courts have approved as complying with the general law and with the Constitution for collecting electronic evidence, storing it and presenting it in court. Only when these procedures are in place will the South African law of electronic evidence be fully effective.

7. CHAPTER 7: INTERNATIONAL INSTRUMENTS AND FOREIGN LAW

7.1 Introduction

In order to assess whether the *Electronic Communications and Transactions Act 25 of 2002* achieves its goal of addressing the handling and the admissibility of electronic evidence, it is important to compare it to foreign legislation. Firstly, the *Electronic Communications and Transactions Act (25 of 2002)* is in most parts based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce with Guide to Enactment (1996).

The *Electronic Communications and Transactions Act (25 of 2002)* complies with the provisions set out in the Model Law, except for the provisions provided on certification as well as electronic signatures (UNCITRAL, 1997).

South Africa became party to the UNCITRAL Model Law on Electronic Evidence by adopting the *Electronic Communications and Transactions Act* (25 of 2002) during 2002. According to UNCITRAL, 54 countries in total have implemented the Model Law or sections of the Model Law in their legislation (UNCITRAL, 1997). Countries, such as Australia, the United Kingdom, the United States of America and Canada also comply with the rules of the Model Law (University of Cape Town & University of Stellenbosch, 286-288).

In this chapter, the Model Law will be discussed, along with the handling of electronic evidence in Australia and Canada.

7.2 The UNCITRAL Model Law

7.2.1 Background

The United Nations Commission on International Trade Law is the legal body of the United Nations, focussing on International Trade Law. One of the UNCITRAL's goals is to provide model law and rules that are acceptable and can be used worldwide.

During meeting of the United Nations General Assembly held on 30 January 1997, it was noted that the prevalence of international trade in an electronic format was increasing (UNCITRAL, 1997). The assembly was furthermore convinced that the implementation of a Model Law could contribute significantly to countries with different legal systems. The assembly furthermore believed that the Model Law on Electronic Commerce would assist countries to revise their current legislation or to formulate legislation where no such

legislation was available. It was recommended that all efforts should be made to make the Model Law on Electronic Commerce known and available to countries (UNCITRAL, 1997).

The UNCITRAL Model Law was adopted in 1996 with an additional article adopted in 1998. Chapter 1 of the Model Law states that: *"*This Law applies to any kind of information in the form of a data message used in the context of commercial activities".

Attached to the Model Law is the *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (2006)* (hereafter Guide to Enactment). The Guide to Enactment stipulates that the purpose of the Model Law can be summarised as follows:

> To offer national legislators a set of internationally acceptable rules as to how a number of such legal obstacles may be removed, and how a more secure legal environment may be created.

The Guide to Enactment further indicated that initially the decision to formalise the Model Law was due to the fact that in various countries the existing legislation addressing the communication and storing of electronic data was insufficient and outdated. In other countries the existing legislation imposed restrictions by requiring electronic evidence to be "written" or *"*original"*.*

7.2.2 The Model Law

Article 5 of the Model Law determines that information will not be denied validity or legal effect purely because such evidence is in the form of a data message.

For the purpose of this study, article 8 of the Model Law is critical, as it addresses the originality of electronic evidence. Based on article 8(1), if law requires that evidence be presented in its original form, that requirement is only met by a data message if it can be reasonable ascertained that the integrity of the data message is kept from the time the evidence was first generated to its final form.

Article 8(3) determines that the criteria for assessing the integrity of the data message will be to establish whether the information in the data message has "remained complete and unaltered", apart from the normal changes during the storing and presenting phases.

Article 9(1) addresses the admissibility of data messages. The article states that during legal proceedings data messages should not be denied admissibility purely because such evidence consists of a data message. It furthermore should not be denied admissibility

on the basis that it is not in its original form if it is the best possible evidence that can reasonably be obtained.

Article 9(2) addresses the evidential weight of data messages. The article states that information captured in the data message must be given due evidential weight. When assessing the evidential weight of a data message, the court must consider the reliability in the manner the data message was created, stored or communicated. The court must furthermore consider the reliability in which the integrity of the data message was maintained, as well as any other relevant factor.

Article 10 determines that the court must be satisfied that the data message remained in the format in which it was "generated, sent or received". If such evidence is retained, it enables the court to identify the origin and the destination of the evidence.

7.2.3 Comparison to the *Electronic Communications and Transactions Act (25 of 2002)*

As per section 233 of the *Constitution of the Republic of South Africa (1996)*, when a court interprets any legislation, the court must "prefer any reasonable interpretation of the legislation that is consistent with international law". The Model Law does not automatically qualify as "international law", as it is not an international agreement. Due to the fact that the Model Law has been utilised or incorporated in various countries, the Model Law is given an international status. The combination of "statement and usage" should provide the Model Law with the required significance of "international law", which could allow for South African courts to interpret the Model Law (Mason, 2007:461).

As seen in Chapter 3 of this study, in comparison with the aforementioned discussion on the Model Law, the *Electronic Communications and Transactions Act (25 of 2002)* and the Model Law are similar and one can see that the *Electronic Communications and Transactions Act (25 of 2002)* was in some part based on the Model Law. Most importantly, the *Electronic Communications and Transactions Act (25 of 2002)* and the Model Law agree on the following (Gereda, 2003:290):

i. The legal requirements of data messages;
ii. The applicability of "writing";
iii. The retention of data messages;
iv. The validity and the development of agreements; and
v. The parties' recognition of data messages.

The Model Law and the *Electronic Communications and Transactions Act (25 of 2002)* do, however, have some differences. They differ slightly on some of the definitions, for example the Model Law defines an intermediary as "a person who, on behalf of another person, sends, receives or stores the data message or provides other services with respect to that data message". The *Electronic Communications and Transactions Act (25 of 2002)* defines an intermediary as "a person who, on behalf of another person, whether as an agent or not, sends, receives or stores that data message or provides other services with respect to that data message"*.*

UNCITRAL recognises that the Model law and the *Electronic Communications and Transactions Act (25 of 2002)* differs in their definition of electronic signatures (UNCITRAL, 1997). The Model Law defines an electronic signature as "data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and indicate the signatory's approval of the information contained in the data message"*.* The *Electronic Communications and Transactions Act (25 of 2002)* defines an electronic signature as "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature"*.* The impact of this difference is that the *Electronic Communications and Transactions Act (25 of 2002)* does not require that the signatory must indicate his/her approval of the information contained in such evidence. The signatory can therefore dispute the evidence as the information contained in the data message may not be accurate. Based on the Model Law, the signatory cannot dispute the data message, as they have approved the data in essence by "signing" it (Gereda, 2003:291).

As the Model Law has been applied in the *Electronic Communications and Transactions Act (25 of 2002)*, it is useful to compare the implementation of the Model Law in other international legislation. For that purpose the legislation of Australia and Canada has been selected as both these countries have implemented the Model Law in their different jurisdictions.

7.3 Australia

Australia differs from South Africa in that it is a federal state, which means that electronic evidence is governed by a Federal Evidence Act, as well as eight different State and Territory Evidence Acts. New South Wales, the Australian Capital Territory and Tasmania have adopted Evidence Acts, which are the same as the Commonwealth Acts. These

acts can be referred to as the *Uniform Evidence Acts*. The *Uniform Evidence Act* indicates that any evidence, which can be produced with or without the help of something else can be considered a document (Mason, 2007:122).

In Victoria, Queensland and South Australia, legislation determines that electronic evidence will be admissible with some conditions. In the remaining states, legislation does not specifically address electronic evidence, but legislation does state that providing a copy, which is identical to the original, will be admissible (Mason, 2007:122).

Section 146 of the *Uniform Evidence Acts* provides a rebuttable presumption that a photocopy or an electronic version of a document can be assumed to be the same as the original. This presumption also speaks to the investigation phase, since detailed logs of modifications are performed on the evidence, as well as encryption to ensure integrity (Mason, 2007:122). Even though this evidence may be admissible, it still may not be reliable and may therefore be given a lower evidential weight. South African legislation also addresses the originality of electronic evidence. The *Electronic Communications and Transactions Act (25 of 2002)* determines that that the court should consider if the information has remained intact. If electronic evidence has been changed, it should have been done in the normal course of collecting, storing and displaying of the evidence. These sections are therefore similar in that proof must be submitted to substantiate the integrity of the electronic evidence.

Section 59 of the *Uniform Evidence Acts* stipulates that if a previous representation was made by an individual, then such evidence would be inadmissible due to hearsay. Section 69 of the *Uniform Evidence Acts*, however, provides an exception rule to hearsay with regard to business records. Hearsay evidence contained in business records will be admissible if such records were captured or generated during the course of business and such records should also have been created for the purpose of the business. When comparing this to the *Electronic Communication and Transaction Act (25 of 2002)*, both allow for an exception rule to hearsay. South Africa, however, differs from Australia in that the *Uniform Evidence Acts* specifies that records should have been created for business purposes, whereas the *Electronic Communications and Transactions Act (25 of 2002)* allows for all records during the normal course of business.

Section 147 of the *Uniform Evidence Acts* furthermore provides a presumption that if copies of business records are tendered, that party would not have to provide evidence

to prove the accuracy of such evidence, unless the opposing party can prove otherwise (Mason, 2007:123).

Another Australian act that regulates electronic evidence is the *Electronic Transactions Act of 1999*. This act is based on the UNCITRAL Model Law. According to the UNCITRAL, the Model Law of 1996 has been implemented in the following Australian jurisdictions (UNCITRAL, 1997):

i. Australian Capital Territory;
ii. New South Wales;
iii. Northern Territory;
iv. Queensland;
v. South Australia;
vi. Tasmania;
vii. Victoria; and
viii. Western Australia.

The *Electronic Transactions Act of 1999*, however, deals primarily with transactions between individuals and the Commonwealth government agencies (Gerada, 286). Since the *Electronic Transactions Act of 1999* is restricted to Commonwealth laws, the Australian territory and state acts would still apply to the statutes, common law and rules of each of the jurisdictions of Australia. The *Electronic Transactions Act of 1999* would therefore not be applicable between private parties (Bolam & Choi, 2012).

The *Electronic Transactions Act of 1999* was introduced to eliminate legal obstacles when identifying electronic documents and digital signatures (Mason, 2007:126). Section 8(1) of the *Electronic Transactions Act of 1999* determines that, for purposes of the Commonwealth, electronic evidence will not be admissible purely because it is by means of electronic communication. Sections 8 to 12 of the *Electronic Transactions Act of 1999* set forth the rules when a person is required to provide information in writing, to produce a document, to record information and how to retain an electronic document (Mason, 2007:126).

The Australian Attorney-General's department states that if any Commonwealth law requires an individual to perform the following, the *Electronic Transactions Act of 1999* allows that individual to perform the tasks electronically:

i. Provide information in writing;

ii. To provide a signature;
iii. To produce a physical document; and
iv. To record and retain information.

As evident from the relevant Australian acts, more provisions are made for the day to day use of electronic tools and documents. In doing so, the legislation is more equipped to address electronic evidence. As electronic evidence is generally admissible in a court of law but the evidential weight has to be determined, more emphasis is placed on the processes before legal proceedings. In other words more emphasis is placed on the processes of gathering, storing and examining the electronic data. It is therefore critical to record each process to provide evidence of the integrity if the electronic evidence (Mason, 2007:123).

7.4 Canada

Canada is a federal state, which means that jurisdiction is divided between the ten provinces and the three territories of Canada. As a result, the federal government of Canada has jurisdiction over criminal law, whereas the other jurisdictions will preside over civil and other matters (Mason, 2007:148).

Canada is a member of the Commonwealth and both federal and provincial governments often referred to as the "crown". Canadian evidence law is mainly from the common law and the common law resides in all the jurisdictions. All the courts in the various jurisdictions will therefore apply more or less the same rules of evidence regardless of province. Each jurisdiction does, however, have its own evidence statutes, which modify the rules of evidence somewhat in that jurisdiction (Mason, 2007:148–149).

Criminal and federal prosecutions are addressed by the *Canada Evidence Act, R.S.C. 1985*. In the last few decades the Canadian Supreme Court has been inclusionary with regard to evidence, unless a policy or an act clearly states otherwise (*R v Corbett [1988] 1 S.C.R. 670 at 691*). Other legislation includes the *Uniform Electronic Commerce Act of 1999*, which is based upon the Model Law (Gerada, 288).

The Canadian courts tend to differentiate between two types of electronic evidence: pure electronic evidence, which is normally used during expert testimony and traditional documentary evidence (Mason, 2007:151).

Canadian law is very clear on the definition of electronic evidence. Section 31.8 of the *Canada Evidence Act, R.S.C. 1985* defines electronic documents as follows:

> Data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data.

Section 5 of the *Uniform Electronic Commerce Act of 1999* determines that electronic evidence will not be denied admissibility purely because such evidence is in an electronic form. This provision is also reflected in both the Model Law and the *Electronic Communications and Transactions Act (25 of 2002)*. According to Article 9(1) of the Model Law, data messages should not be denied admissibility purely because such evidence consists of a data message. Section 15(1) of the *Electronic Communications and Transactions Act (25 of 2002)* determines that rules of evidence should not be applied so that a data message is not admissible purely because such evidence constitutes a data message.

One way to compare international legislation is to compare the challenges that both countries face. As discussed in Chapter 5 of this study, the challenges that electronic evidence faces in South Africa are mainly hearsay, originality, authenticity and reliability. The Uniform Law Conference of Canada (ULCC) found that the difficulties with electronic evidence were found between the following three aspects of electronic evidence:

i. Hearsay: Once a document is adduced to prove the contents thereof, such document will be considered as hearsay;
ii. Authenticity: In order to admit a document, evidence must be provided to prove the authenticity thereof; and
iii. Best evidence rule: If an individual relied on a document, the original of that document must be provided. If an original document cannot be admitted the individual must satisfy the court that a copy of the document is reasonable.

Section 31.1 of the *Canada Evidence Act, R.S.C. 1985* addresses the authenticity of electronic documents. The act determines that if any individual is seeking to admit an electronic document, the onus is on that individual to prove the authenticity of such a document. The authenticity can be proved by “evidence that is capable of supporting a finding that the electronic document is that what it is purported to be”.

As indicated above, another hurdle that electronic evidence faces in Canada is the best evidence rule. Traditionally the rule was created for parties to prove the integrity of the electronic documents. The integrity of such documents could be proven by either providing original documents or proving that a copy was created in a trustworthy manner. The integrity of the electronic document can also be proved through an affidavit, but in some instances expert testimony would then be required. In South African legislation, the general rule of originality also applies to electronic evidence. Section 14(1) of the *Electronic Communications and Transactions Act (25 of 2002)* determines that if law requires evidence to be in its original form, a data message will meet this requirement if it can be proven that the integrity of the data message has been maintained and therefore remained unaltered. Section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* furthermore states that if the data message is the best evidence, it may be admissible even if such a data message is not in its original form.

The *Uniform Electronic Evidence Act of 1999* provides further measures to determine the integrity of electronic documents. The integrity of electronic documents can be established through either of the following (Mason, 2007:153):

i. By proving that the computer or other storage medium was working properly;
ii. By proving that the electronic document was "recorded or stored, recorded and stored" by an adverse individual; or
iii. By proving that the electronic document was generated or stored during the normal course of business by an individual not part of the proceedings.

Section 31(2) of the *Canada Evidence Act R.S.C. 1985* states, despite the requirements of authenticity in section 31(1), the following:

> An electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information or stored in the printout.

The third hurdle with regard to electronic documents is hearsay. According to the ULCC, the exception rules of hearsay that normally apply to electronic documents are the exception rule on business records and the general exception rule. The exception rule of business records determines that if the electronic document was created during the normal course of business and the document is relied on in the business then such a document will be admissible. In South Africa, the *Criminal Procedure Act (51 of 1977)*

and the *Electronic Communications and Transactions Act (25 of 2002)* also allow for documentary evidence that was created during the normal course of business.

The general hearsay exception rule is that if it can be proven that the evidence of the content of the document is reliable and the evidence is necessary for the purpose of determination of the issue, such evidence will be admissible. The ULCC determined that the rules of hearsay evidence were sufficient to address hearsay evidence and was therefore of the opinion that no change to the rules of hearsay was necessary.

7.5 Conclusion

It is apparent that there are similarities between the *Electronic Communications and Transactions Act (25 of 2002)* and the Model Law, as well as other legislation. It is also evident that the challenges that electronic evidence faces are not only limited to South Africa.

8. CHAPTER 8 : CONCLUSION

What is the impact of electronic evidence during a forensic accounting investigation? This was the problem statement raised in Chapter 1 at the commencement of this study and a response was obtained throughout Chapters 2 to 7.

8.1 The forensic accountant

In order to determine what the impact of electronic evidence in forensic accounting investigations is, one needs to understand what a forensic accountant is and what a forensic accountant does.

Worldwide, law enforcement has come to the realisation that to solve economic crimes, financial information is necessary. Law enforcement, however, does not have the technical skills and knowledge to effectively deal with technical and financial information (Manning, 2004:515). Myburgh J made the following comment in the case of *S v Botha and others 1995 2 SACR 598 W*, which summarises the need for forensic accountants perfectly:

> Society has become so specialized and there are so many laws and activities that need to be administered and regulated, that no police service can investigate and prevent all crime in a modern society without the help of private investigators.

By obtaining input from various sources, the basic skills set of the forensic accountant can be summarised as follows:

i. Legal knowledge in both civil and criminal proceedings;
ii. Accounting knowledge;
iii. Investigative skills;
iv. Interviewing skills;
v. Information technology and data analytic skills; and
vi. The ability to testify during legal proceedings.

In order to understand the role and the responsibility of the forensic accountant, it was also essential to understand how the forensic accountant is regulated. In later years, the forensic accountant has been regulated, which gives the profession a higher regard in courts of law. The forensic accountant is regulated by the ICFP and the ACFE.

The more the industry and the courts recognise the need for the specialised services of the forensic accountant, the more reliance will be placed on forensic accounting investigations during legal proceedings.

8.2 Historical overview of legislation

As stated in Chapter 1 of this study, certain secondary questions were to be answered throughout the study in order to address the problem statement. The first secondary question was how legislation developed in South Africa with regard to electronic evidence. The following legislation was applicable to electronic evidence:

i. *The Criminal Procedure Act (51 of 1977);*
ii. *The Law of Evidence Amendment Act (45 of 1988);*
iii. *The Civil Proceedings Evidence Act (25 of 1965);*
iv. *The Computer Evidence Act (57 of 1983); and*
v. *The Electronic Communications and Transactions Act (25 of 2002).*

8.2.1 The Criminal Procedure Act (51 of 1977)

Section 221(5) of the *Criminal Procedure Act (51 of 1977)* aims to define a "document" to include the apparatus on which the information can be stored or recorded. Case law, however, determined that if the computer was used for more than simply storing the information, such evidence would not be admissible in terms of section 221 of the *Criminal Procedure Act (51 of 1977).*

Since the *Criminal Procedure Act (51 of 1977)* only allows for certain types of electronic documents and also only evidence that was stored on the computer, it was essential to consider the development of other legislation.

8.2.2 The Law of Evidence Amendment Act (45 of 1988)

The general rule of hearsay is that hearsay in not admissible due to the fact that the evidential value of such evidence depends on the testimony of an individual not testifying. Section 3 of the *Law of Evidence Amendment Act (45 of 1988)* allows for the court's discretion to allow hearsay evidence. The *Law of Evidence Amendment Act (45 of 1988)* is therefore essential when considering the admissibility of electronic evidence.

8.2.3 The Civil Proceedings Evidence Act (25 of 1965)

The *Civil Proceedings Evidence Act (25 of 1965)* allows for the relaxation of the hearsay rule. Section 34(1) of the *Civil Proceedings Evidence Act (25 of 1965)* states that in instances where oral evidence would be admissible in a civil case, a statement made by an individual, in the form of a document, would also be admissible if the original document was submitted. The *Civil Proceedings Evidence Act (25 of 1965)*, however, also stipulates that the individual who made the statement is to testify during the proceedings, with the some exceptions

8.2.4 The Computer Evidence Act (57 of 1983) (repealed)

The *Computer Evidence Act (57 of 1983)* determined that a certified computer printout would have been admissible if the facts contained in the computer printout would have been admissible if tendered as direct, oral evidence (Schwikkard & Van der Merwe, 2009:444). Challenges were experienced with the compliance of the act due to the excessive technical requirements of the *Computer Evidence Act (57 of 1983)* (Schwikkard & Van der Merwe, 2009:445).

The *Computer Evidence Act (57 of 1983)* was therefore not the solution to the issues facing electronic evidence, and the need once again arose for new legislation.

8.2.5 The Electronic Communications and Transactions Act (25 of 2002)

The final legislation to consider is also the latest legislation. As the *Computer Evidence Act (57 of 1983)* was deemed to lack the proper elements to deal with electronic evidence, the *Electronic Communications and Transactions Act (25 of 2002)* was introduced. The *Electronic Communications and Transactions Act (25 of 2002)* moves away from the concept of “computer printouts” and focuses more on terms, such as “data messages”.

Section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* states that law of evidence should not deny the admissibility of data messages on the mere grounds that it is a data message. The exact meaning of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* is, however, unclear. Does the *Electronic Communications and Transactions Act (25 of 2002)* intend for all electronic evidence considered to be hearsay evidence to be admissible? In the case of *Ndlovu v Minister of Correctional Services & Another 2004 JDR 0328 (W)* the judge was not

willing to allow the evidence in terms of the *Electronic Communications and Transactions Act (25 of 2002)* and stated that:

> *Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving the evidence, there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence.*

The *Electronic Communications and Transactions Act (25 of 2002)* is considered the most recent legislation to address electronic evidence, but still the courts would rather rely on earlier legislation that addresses documentary evidence and hearsay evidence. If the court does not place any reliance on the *Electronic Communications and Transactions Act (25 of 2002)*, then the purpose of the act should be determined. The challenge of relying only on earlier legislation is that such evidence also has its own set of challenges. The *Criminal Procedure Act (51 of 1977)* deals mostly with business records, whereas the *Law of Evidence Amendment Act (45 of 1988)* and the *Civil Proceedings Evidence Act (25 of 1965)* address mostly hearsay evidence.

The results of the SALRC's discussion paper into electronic evidence may have a significant influence on legislation going forward. Once the paper has been issued, it may either require that further research be undertaken or it may shed light on the issues and the purpose of the *Electronic Communications and Transactions Act (25 of 2002).*

The mere fact that challenges with electronic evidence persist, supports the finding that South African legislation is not fully equipped to deal with electronic evidence.

8.3 Electronic evidence

Before assessing the impact of electronic evidence in forensic accounting investigations, it was necessary to ascertain what type of evidence electronic evidence is. In order to meet this secondary objective, one had to consider the traditional forms of evidence, which are:

i. Documentary evidence;
ii. Real evidence; and
iii. *Viva voce* evidence.

Electronic evidence can further be divided into three categories:

i. Documents or files that contain content have been written or created by one or more people;
ii. Records that have been generated by a computer and where there is no human interference or input; and
iii. Records that consist of both inputs generated by a computer and human inputs. (Mason, 2007:xiii).

For the purpose of this study documentary evidence, real evidence and evidence as the product of an apparatus was considered.

8.3.1 Documentary evidence

Electronic evidence can be considered as documentary evidence and therefore has to comply with the requirements of documentary evidence. In order for a document to be admissible in a court of law, the documentary evidence is subjective to three general rules:

i. The document must be produced;
ii. The contents of the document can be proved by the production of the **original** document;
iii. Evidence is required to prove the **authenticity** of the document (Mason, 2007:464); and
iv. The document may have to be stamped if so required by the *Stamp Duties Act 77 of 1968* (Zeffertt *et al*., 2003:685).

These general rules are, with the exception of hearsay, the biggest issues facing electronic evidence. The challenge arises because a computer printout is not considered to be the original document. If the document was scanned into the computer then the scanned document on the computer would be a copy. If the document was created on the computer, then the original would be on the computer hard drive and the computer printout would be the copy. Even then the origins of the original document would be hard to determine due to the fact that electronic documents can easily be altered.

8.3.2 Real evidence

If a document is submitted to prove the contents thereof, such documents would be considered to be documentary evidence. If the document is, however, submitted purely as an object, such evidence would be considered to be real evidence (Schmidt & Rademeyer, 1989:326). Real evidence differs from documentary evidence in that real evidence is always admissible if it is relevant and meaningful (Schmidt & Rademeyer 1989:326).

If a computer was therefore solely responsible for electronic evidence, with no human input, such evidence could be considered as real evidence. If part of the evidence was, however, due to human input, normal hearsay rules would apply.

8.3.3 Evidence as the product of an apparatus

Evidence as the product of an apparatus is usually divided between documentary evidence and real evidence (Schutte 2009: 104). Like with documentary evidence, evidence as a product on an apparatus, should also be disclosed and the authenticity thereof should be proven. When disclosing the type of apparatus used, it is important to prove that it is reliable. It should therefore be verified that the computer is a reliable instrument for the purpose for which it is being used (Schutte, 2009:104).

The fact that electronic evidence can be either of the aforementioned types of evidence furthermore creates challenges for electronic evidence. The impact thereof is that the court firstly has to determine in which category of evidence electronic evidence falls. There is therefore no golden rule as to the type of evidence that electronic evidence is.

8.4 Issues facing electronic evidence

In order to assess the role of the forensic accountant during forensic accounting investigations, the forensic accountant should be aware of the admissibility obstacles that electronic evidence faces during legal proceedings.

The legal issues that were discussed in this study were:

i. Hearsay evidence;
ii. Originality;
iii. Authenticity; and
iv. Reliability.

8.4.1 Hearsay evidence

When determining what type of evidence computer evidence is, the first and most important step is to determine for what purpose the computer or electronic apparatus was used. Was the computer used to simply store information? Was the information on the computer captured by an individual or did the computer process information without or with human input?

Section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* states that law of evidence should not deny the admissibility of data messages on the mere grounds that it is a data message. If further states that if the evidence is the best evidence that could or could reasonably be expected to be obtained, the evidence should not be denied on the grounds that it is not in its original form. It is unclear whether the purpose of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* is to allow for all hearsay evidence to be admissible.

Legislation is still unclear on how electronic evidence should be dealt with if deemed hearsay. Once issued, the Issue Paper 27 on electronic evidence by the SALRC may provide valuable insight into how to address electronic evidence if deemed hearsay evidence.

8.4.2 Originality

One of the requirements of documentary evidence to be admissible is that the original document has to be presented. The inherent challenge with electronic evidence is that it is in most instances not the original. Legislation, however, provides clear guidance as to when a copy of the original document may be admissible. *The Electronic Communications and Transactions Act (25 of 2002)* also requires for evidence to be in its original form. The *Electronic Communications and Transactions Act (25 of 2002)*, however, allows for

the best evidence to be admissible. Legislation therefore appears to be adequate to address the issue of the originality of electronic evidence.

8.4.3 Authenticity

The general rule is that the party who tenders documentary evidence also has to adduce evidence to prove to the court that the document is authentic. The proof of authenticity creates various issues for electronic evidence. In many instances the author will be unknown or a document will have various authors. If the author can be identified, the documents authenticity is still in question for the following reasons:

i. The author merely captured the information with which he/she was provided;
ii. The information provided could have been incorrect;
iii. The author could have captured the information incorrectly; and
iv. Computer evidence is easily altered or deleted.

As with hearsay evidence, the purpose of the *Electronic Communications and Transactions Act (25 of 2002)* with regard to authenticity is unclear. As the *Electronic Communications and Transactions Act (25 of 2002)* allows for best evidence to be admissible, it may result in evidence that is the best evidence to be admissible even it such evidence is not proved to be authentic.

8.4.4 Reliability

The proof of reliability also stems from the proof of relevancy, since only a product from a reliable apparatus can provide evidence from which a reasonable conclusion can be drawn. It is not always solely the reliability of the computer itself that is in question. The reliability of the operator of the computer may also be in dispute.

Reliability also comes into question with hearsay evidence. One of the reasons hearsay evidence is not admissible, is that hearsay evidence is not reliable. If the purpose of section 15 of the *Electronic Communications and Transactions Act (25 of 2002)* is to allow hearsay evidence, it might result in admitting electronic evidence that is not reliable. This further reiterates the need for clarity on section 15 of the *Electronic Communications and Transactions Act (25 of 2002)*.

8.5 The collection and storage of electronic evidence

In order to determine the impact of forensic accounting investigations, the forensic accountant has to perform the investigation always considering the impact thereof during legal proceedings. The investigation should therefore be performed in such a manner that the evidence will be admissible in a court of law. No set guidelines on how to collect, to store and to analyse electronic information are provided by the courts.

Based on research in Chapter 6 of this study, the following can be considered as a potential guideline on how to practically deal with electronic evidence during forensic accounting investigations:

i. **Collection phase:** The location and the various forms of electronic media should be determined in advance in order to specify what information is required. The forensic accountant collecting the electronic evidence should be duly authorised to do so. Care should be taken to ensure that the integrity of the evidence stays intact;
ii. **Preserving and authentication phase:** The integrity, the origins and then authenticity of the electronic evidence should be determined. The forensic accountant should furthermore ensure that the information cannot be altered or modified;
iii. **The analysing or examination phase:** The electronic evidence should be analysed by the forensic accountant. The forensic accountant should document all the steps performed on the data, as well as the methods that were applied. An unbiased third party should be able to come to the same conclusion as the forensic accountant;
iv. **Presenting:** The forensic accountant should be able to present the evidence, as well as the findings to a court of law. The evidence should therefore be in a presentable format. The forensic accountant should also be able to testify during legal proceedings.

It is recommended that the courts provide guidelines on how to collect, to store and to analyse electronic evidence. Only once these guidelines have been put in place will the forensic accountant, the South African Police Service and the courts have clarity on what is expected of electronic evidence.

8.6 International instruments and foreign law

It is evident that even though the UNCITRAL Model Law served as a reference for the legislation in South Africa, Australia and Canada, the legislation of the different countries differs in some ways. The *Electronic Communications and Transactions Act (25 of 2002)* was modelled on the UNCITRAL Model law and it is apparent that the *Electronic Communications and Transactions Act (25 of 2002)* does have similarities with other international legislation.

What is also clear, is that the issues facing electronic evidence are not only limited to South Africa. Other countries also face the issues of hearsay, authenticity and best evidence. This seems to imply that maybe electronic evidence will always inherently be problematic and that legislation will potentially always struggle with electronic evidence.

8.7 Conclusion

The impact of electronic evidence in forensic accounting investigations remains problematic. The forensic accountant faces various challenges during a forensic accounting investigation.

The legislation that should assist the forensic accountant during investigations was found to be lacking and unclear. The inherent challenges that electronic evidence faces are not always addressed in the legislation.

Lastly, no set guidelines are provided to forensic accountants during forensic accounting investigations and therefore forensic accountants have drafted their own guidelines for the collection and storage of electronic evidence. The aforementioned challenges should be re-evaluated once the SALRC issue the findings of Paper 27, which would hopefully address the issues facing electronic evidence.

9. BIBLIOGRAPHY

Acts ***see*** South Africa

Anon. 2010. Defining the South African Forensic Accountant. *Accountancy SA.* [Web:] http://www.accountancysa.org.za/resources/ShowItemArticle.asp?Article=%3Cb%3EDefining+the+South+African+Forensic+Accountant+%3C%2Fb%3E&ArticleId=1896&Issue=1090#comments [Date of access: 11 April 2013].

Association of Certified Fraud Examiners. 2013. [Web:] http://www.acfe.com/forensic-accountant.aspx [Date of access: 25 October 2012].

Association of Certified Fraud Examiners. South African Charter. 2013. [Web:] http://www.acfesa.co.za/about-us/acfe-sa-fact-sheet/ [Date of access: 11 June 2013].

Association of Chief Police Officers. 2011. Good Practice Guide for Computer-Based Electronic Evidence. [Web:] http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf [Date of access: 15 October 2013].

Australia 1999 Electronic Transactions Act of 1999

Australia Uniform Evidence Acts

Australian Attorney-General's Department. 2013. [Web:] http://www.ag.gov.au/RightsAndProtections/ECommerce/Pages/default.aspx [Date of access: 23 October 2013].

Basdeo, V. 2012. The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis. *South African Journal of Criminal Justice,* 25(2):195-212.

Bellengére, A. *et al.* 2013: The Law of Evidence in South Africa: Basic Principles. Cape Town: Oxford University Press South Africa.

Bolam, P. and Choi, R. 2012. Electronic Signatures: When are they effective? [Web:] http://www.google.com/url?q=http://www.qls.com.au/files/70592b75-748f-44df-a1bd-a1e400a3397f/Electronic_signatures_when_effective.pdf&sa=U&ei=k2V-UtrmG6un0wWpzYD4Ag&ved=0CBEQFjAC&sig2=7vD2Rt8f_Hj2ir1sgnhjcw&usg=AFQjCNHImAT1bOhoLhFIHtazpPJfCdcuwQ [Date of access: 23 October 2013].

Canada 1985. Canada Evidence Act, R.S.C. 1985.

Canada 1988. R v Corbett [1988] 1 S.C.R. 670 at 691.

Canada 1999 Uniform Electronic Commerce Act of 1999.

Canadian Institute of Chartered Investigators. 2013. [Web:] http://www.cica.ca/focus-on-practice-areas/forensic-accounting/item61435.aspx [Date of access: 31 May 2013].

Casey, E. 2002. Digital Evidence and Computer Crime: Forensic Science, computers and the internet. Florida: Academic Press.

CCS South Africa. 2011. [Web.] http://www.csione.com/index_files/ComputerForensics.htm [Date of access: 10 October 2011].

CHARTERED INSTITUTE OF MANAGEMENT ACCOUNTANTS. 2014 [Web:] http://www.cimaglobal.com/Our-locations/Africa/South-Africa/ [Date of access: 27 March 2014]

Collier, D. 2005. Evidently not so simple. *Juta's Business Law,* 13(1):6-9.

Constitution ***see*** South Africa

Crumbley, D., Larry, Heitger, Lester, E. & Smith, G. Stevenson. 2007: Forensic and investigative accounting 3rd ed. North Ryde, Australia: CCH

Deloitte. 2013. [Web:] http://www.deloitte.com/view/en_ZA/za/services/riskadvisory/forensics/index.htm [Date of access: 29 October 2013].

De Villiers, D. 2012. Adequacy of SA Law: Electronic Evidence. De Villiers made this presentation during the 2012 ICFP Conference. [Web:] http://www.icfp.co.za/sites/default/files/Dawie%20de%20Villiers%20-%20Adequacy%20of%20SA%20Law%20-%20Electronic%20Evidence.pdf [Date of access: 7 October 2013].

Electronic Discovery Reference Model. 2009. [Web:] http://www.edrm.net/what-is-edrm [Date of access: 14 October 2013].

Ernest & Young. 2013. [Web:] http://www.ey.com/ZA/en/Services/Assurance/Fraud-Investigation---Dispute-Services [Date of access: 22 May 2013].

Gereda, Shumani L. 2003. Electronic Communications and Transactions Act [Web:] http://www.google.com/url?q=http://thornton.co.za/resources/telelaw12.pdf&sa=U&ei=7WB-Upa4IcfW0QWlkIHwCQ&ved=0CAsQFjAA&sig2=vsm46kPFhQJQ1sH4F1wgBA&usg=AFQjCNFU-ZFAH75M4bWTdfFdUr7usXT-KA [Date of access: 9 November 2013].

Hershensohn, J. 2005. I.T. Forensics: The Collection and Presentation of Digital Evidence. [Web:] http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf [Date of access: 14 October 2013].

Hübschle, A. The South African Crime Bureau. [Web:] http://www.saicb.co.za/ [Date of access: 26 July 2011.]

Institute of Commercial Forensic Practitioners. 2011. [Web:] http://www.icfp.co.za/our-mission-vision-values [Date of access: 31 May 2013].

Interpol. 2011. INTERPOL Forensic Science Symposium. [Web:] http://134.50.70.12/Publications/wyndrose/CASMAT/EVID/INTPL.pdf [Date of access: 15 October 2013].

KPMG. 2013. [Web:] http://www.kpmg.com/ZA/en/WhatWeDo/Advisory1/Risk-Consulting/Forensic/Pages/default.aspx [Date of access: 22 May 2013].

KPMG. 2013. 3rd Africa Fraud Barometer. [Web:] http://www.google.com/url?q=http://www.kpmg.com/Africa/en/IssuesAndInsights/Articles-Publications/Documents/3rd%2520KPMG%2520Africa%2520Fraud%2520Barometer%2520-%2520January%25202013.pdf&sa=U&ei=E2l-Us2yOseX1AXUioHwBw&ved=0CAsQFjAA&sig2=0Ge0CK085jLqhgMLgqZUWA&usg=AFQjCNG1OuUXJScsjYIY6Mlbq46Kpa5RRw [Date of access: 9 November 2013].

Law Reports ***see*** South Africa

Levine, Curry, Sobel, Gilgoff, Mulrine, Pethokoukis, Morris. 2002. Careers to count on. *U.S. NEWS.* 2 October 2002.

http://www.usnews.com/usnews/biztech/articles/020218/archive_020208.htm [Date of access: 7 November 2013].

Manning, G.A. 2005. Financial Investigation and Forensic Accounting. 2nd edition. Florida: CRC Press.

Mason, S. 2007. Electronic Evidence: Disclosure, Discovery & Admissibility. LexisNexis Butterworths.

Network of Independent Forensic Investigators. 2011. [Web:] http://www.nifa.co.uk/forensic-accounting.cfm [Date of access: 22 May 2013].

PricewaterhouseCoopers, 213. [Web:] http://www.pwc.co.za/en/forensic-investigations-and-dispute-resolution/index.jhtml [Date of access: 14 October 2013].

Sargant, B. 2013. Training to be a contender in forensic accounting. Have a well-rounded repertoire. [Web:] http://www.cica.ca/focus-on-practice-areas/forensic-accounting/conversations-about-forensic-accounting/entries/item73968.aspx [Date of access: 31 May 2013].

Schmidt, C.W.H. & Rademeyer, H. 1989. Bewysreg. 4de ed. Durban: LexisNexis Butterworths.

Schutte, F. 2010. Evidence Law (JURI 325). Potchefstroom: North-West University.

Schwikkard, P.J. & Van der Merwe, S.E. 2009. Beginsels van die Bewysreg. 2de ed. Juta Law Publishers.

Shachtman, N. 2011. The Washington Post. [Web:] http://web.ebscohost.com.nwulib.nwu.ac.za/ehost/detail?sid=7da7546e-aebf-43a8-b6e3-

a9860850a610%40sessionmgr4&vid=1&hid=18&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=nfh&AN=wapo.99d503c2-b3fd-11e0-a764-912ca2193644 [Date of access: 25 July 2011].

South Africa. 1988. Amended Law of Evidence Amendment Act 45 of 1988.

South Africa. 1982. Barclays Western Bank Ltd v Creser 1982 (2) SA 104 (T).

South Africa. 2007. Beheersmaatschappij Helling I NV and others v Magistrate, Cape Town, and Others 2007 (1) SACR 99 (C).

South Africa. 1973. Chopra v Sparks Cinemas (Pty) ltd and Another 1973 (2) SA 352 (D).

South Africa. 1966. Civil Proceedings Evidence Act 25 of 1965.

South Africa. 1983. Computer Evidence Act 57 of 1983.

South Africa. 1996. Constitution of the Republic of South Africa 1996.

South Africa. 1977. Criminal Procedure Act 51 of 1977.

South Africa. 2002. Electronic Communications and Transactions Act 25 of 2002.

South Africa. 1924. Estate De Wet v De Wet 1924 CPD 341.

South Africa. 1998. Ex parte Rosch (1988) 1 All SA 319 (W).

South Africa. 2004. Extra Dimension and others v Kruger NO and others 2004 (2) SACR 493 (T).

South Africa. 1938. Fischer v R 1938 2 PH 044 (O).

South Africa. 1981. Knouwds v Administrateur, Kaap 1981 1 SA 544 (K).

South Africa. 1976. Narlis v South African Bank of Athens 1976 2 SA 573 (A) 577H.

South Africa. 2005. Ndlovu v Minister of Correctional Services & Another 2005 JDR 0328 (W).

South Africa. 1908. R v Daye 1908 2 KB 333 340.

South Africa. 1975. S v Bornman 1975 1 SA 658 (T).

South Africa. 1995. S v Botha and others 1995 2 SACR 598 W.

South Africa. 1976. S v Claassen 1976 2 SA 281 (O).

South Africa. 1981. S v Harper 1981 (1) SA 88 D.

South Africa. 1964. S v Margolis 1964 4 SA 579 (T) 582.

South Africa. 2002. S v Mashiyi 2002 (2) SASV 387 (Tk).

South Africa. 1986. S v Mpumlo and Others 1986 (3) SA 485 (E).

South Africa. 1970. S v Mutle 1970 4 SA 535 (T) 537.

South Africa. 2008. S v Ndiki 2008 (2) SASV 252.

South Africa. 1977. S v Pennels 1977 1 SA 809 (N).

South Africa. 1996. S v Ramavhale 1996 1 SASV 639 (A).

South Africa. 2005. S v Shaik and others [2005] 3 All SA 211 (D).

South Africa. 1972. S v Smuts 1972 4 (SA) 358 (T).

South Africa. 1919. Seccombe v Attorney-General 1919 TPD 270 277.

South Africa. 1973. South African Law Reform Commission Act 19 of 1973

South Africa. 1968. Stamp Duties Act 77 of 1968.

South Africa. 1958. Police Act 7 of 1958.

South Africa. 1919. Watts and Darlow v R 1919 NPD.

Van der Merwe, D. 2002. Computers and the Law. Juta.

Van Romburgh, J.D. 2008. The training of a forensic accountant in South Africa. Potchefstroom: NWU. (Mini-dissertation – MCom).

Van Rooyen, H.J.N. 2004. Investigation: The A-Z Guide for Forensic, Private and Corporate Investigations. Crime Solve.

South African Law Reform Commission. 2007. [Web:] http://www.justice.gov.za/salrc/ [Date of access: 14 October 2013].

Timmer, M. 2011. Getting the most out of s11D. *Without Prejudice*, 11(2):57-58.

THE SOUTH AFRICAN INSTITUTE OF CHARTERED ACCOUNTANTS. 2008 [Web:] https://www.saica.co.za/ [Date of access: 27 March 2014]

THE SOUTH AFRICAN INSTITUTE OF GOVERNMENT AUDITORS. 2014 [Web:] http://www.saiga.co.za/home.htm [Date of access: 27 March 2014]

THE SOUTH AFRICAN INSTITUTE OF PROFESSIONAL ACCOUNTANTS. 2014 [Web:] http://www.saipa.co.za/ [Date of access: 27 March 2014]

Uniform Law Conference of Canada. 1997. [Web:] http://www.ulcc.ca/en/1997-whitehorsef-yt/377-civil-section-documents/360-electronic-evidence-act-consultation-paper?showall=&start=2 [Date of access: 23 October 2013].

United Kingdom. 1968. The Statue of Liberty [1968] 2 All ER 195.

United Nations Commission on International Trade Law. [Web:] http://www.uncitral.org/uncitral/en/index.htm [Date of access: 13 October 2011].

United Nations Commission on International Trade Law.. Model Law [Web:] http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html [Date of access: 13 October 2011].

United States. 2009. Federal Rules of Evidence.

University of Cape Town, Student Law Society. University of Stellenbosch, Student Law Society. 2006: Responsa meridiana.

Zeffertt, D.T., Paizes, A.P. and Skeen, A.St.Q. 2003. The South African Law of Evidence. Durban: LexisNexis.