EXPLORING THE VALUE OF COMPUTER FORENSICS IN THE INVESTIGATION OF PROCUREMENT FRAUD

by

ALUWANI RUFAROH THEMELI

Submitted in accordance with the requirements for the degree

MAGISTER TECHNOLOGIAE

in the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROF J.G. VAN GRAAN

CO-SUPERVISOR: MR B.K. LEKUBU

JANUARY 2017

DECLARATION

Student Number: 34165177

I declare that the thesis *"Exploring the value of computer forensics in the investigation of procurement fraud"* is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

I further declare that this study has not previously been submitted for any degree or examination at any other university.

Aluwani Rufaroh Themeli

Signed at, Pretoria, South Africa, January 2017

DEDICATION

This thesis is dedicated to:

My late father

Ntshengedzeni Archiebold Themeli

20 April 1957 – February 1979

and

My late grandmother

Alilali Nthatheni Takalani Themeli

04 June 1925 – 23 October 2014

Vhakololo vha Mukula la Vho-Takalani na Ngwenani ya ha-Themeli Mugo wa Shango, la Vho Muthu ha thonwi hu thonwa Mbudzi na Kholomo, edelani nga mulalo.

I will not forget you, i will not dishonor you, I will not forsake you, i will remember and be glad that you raised me, taught me, guide me and that you loved me always.

Ndaa

ACKNOWLEDGEMENTS

There were many people who have contributed immensely to the successful completion of this dissertation. I would like to take this opportunity to convey my sincere and heartfelt gratitude to the following people:

- My Heavenly Father, Almighty God, for all the blessings and energy. His glory and gravitas will triumph over all of creation for eternity.

- My supervisor, Prof J.G. van Graan, and my co-supervisor, Mr B.K. Lekubu, for their continuous encouragement, guidance and persistent support throughout my studies.

- Mr Obed Thenga (Chief Audit Executive, City of Tshwane) for granting me approval to conduct the research with the City of Tshwane, Forensic Services.

- All my colleagues and friends for their constant support.

- A special “thank you” to my family, especially my son, Jermaine Themeli, for their patient love, support and understanding during demanding times.

ABSTRACT

The research problem for this study was that forensic investigators in the Forensic Services (FS) of the City of Tshwane (CoT) are unable to successfully deal with procurement fraud as a result of the lack of knowledge, skills and resources required to conduct computer forensics during the investigation of procurement fraud. This research was conducted to ascertain the value of computer forensics in the investigation of procurement fraud. Further, the study sought to determine how to improve the CoT forensic investigators' knowledge and competence regarding the application of computer forensics in the investigation of procurement fraud.

The purpose of this study was to explore the procedures that should be followed by CoT forensic investigators when conducting computer forensics during the investigation of procurement fraud. The research also aimed to discover new information, not previously known to the researcher, related to computer forensics during the investigation of procurement fraud by exploring national and international literature. In addition, the study explored existing practices so as to use this information to improve the current CoT procedure, within the confines of the legislative requirements.

The overall purpose of this study is to provide practical recommendations for best practices, based on the results of the data analysis, which address the problem and enhance the investigative skills of CoT forensic investigators. The study established that it is imperative and compulsory to apply computer forensics in any procurement fraud investigation in order to efficiently track down cyber criminals and solve complicated and complex computer crimes. It was also established that forensic investigators within the FS in the CoT lack the necessary computer skills to optimally investigate procurement fraud. It is therefore recommended that CoT forensic investigators acquire the necessary skills and essential training in computer forensics in order to improve their knowledge and competence regarding the application and understanding of the value of computer forensics in the investigation of procurement fraud.

KEY TERMS

Forensic investigation; Computer forensics; Procurement fraud; Computer investigation; Red flags; Computer evidence; Network forensics; Kickbacks; Bid rigging; Conflict of interest.

LIST OF ABBREVIATIONS

ACFE	-	Association of Certified Fraud Examiners
CFE	-	Certified Fraud Examiners
BTech	-	Baccallaureus Techonologiae
CATTs	-	Computer Assisted Auditing Techniques
CD	-	Compact Disc
CD-ROM	-	Compact Disc Read only Memory
CMOS	-	Complementary Metal-oxide Semiconductor
CoT	-	City of Tshwane
CRC	-	Cyclic Redundancy Check
DAT	-	Digital Audio Tape
DVD	-	Digital Versatile Disc
EC-Council	-	International Council of Electronic Commerce Consultants
FS	-	Forensic Services
FTK	-	Forensic Toolkit
GAR	-	Group Audit and Risk Department
ICT	-	Group Information & Communication Technology Management
IT	-	Information Technology
IP	-	Internet Protocol

MAYCO	-	Mayoral Committee
MD5	-	Message-digest Algorithm
MFMA	-	Municipal Finance Management Act
MS	-	Microsoft
NTPASS	-	Novell NetWare Password Recovery Program
PC	-	Processing Computer
PDA	-	Personal Digital Assistant
RAID	-	Redundant Array of Independent Disks
RAM	-	Random Access Memory
SAPS	-	South African Police Service
SCM	-	Supply Chain Management
SIU	-	Special Investigation Unit
SVGA	-	Super Video Graphic Array
UNISA	-	University of South Africa
USB	-	Universal serial bus
VGA	-	Video Graphic Array
WDPASS	-	Access Data Password Recovery Program for Microsoft Word
WORM	-	Write Once, Read Many

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ANNEXURES

CHAPTER ONE
GENERAL ORIENTATION

1.1 INTRODUCTION

Computer forensics has become increasingly essential for the successful investigation of procurement fraud and the effective prosecution of perpetrators committing such an offence. It involves an analysis of diverse digital devices such as computer system devices, network devices, mobile devices and storage devices. According to Maras (2015:29), computer forensics is the process of obtaining, processing, analysing, and storing digital information for use as evidence in criminal, civil, and administrative cases. Evidence retrieved and obtained must be admissible in a court of law and disciplinary proceedings. Therefore, for computer forensics to be performed successfully, there are a number of important steps that have to be taken into consideration (Maras, 2015:34).

According to Sammes and Jenkinson (2013:1), computer forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and the law. In computer forensics investigative practice, there are hundreds of computer forensic investigation procedures developed the world over to deal with procurement fraud. However, each organisation tends to develop its own procedures, and some focus on technological aspects such as data acquisition or data analysis (McCombie & Warren, 2003:10).

In the CoT, procedure requires that a computer involved in the commission of fraud will be seized and taken to the Department of Group Information & Communication Technology Management (ICT) for data retrieval. The data will be safely preserved for analysis. Data analysis will be conducted for its relevancy to the investigation, either by an internal forensic investigator or by outsourcing the services of a panel of external service providers. A forensic report will be compiled and approved by the FS management. The final stage of this process is a presentation of the findings to the relevant department or process owners, and to testify in disciplinary proceedings or in a court of law, if required to do so.

1.2 BACKGROUND HISTORY

“The City of Tshwane Metropolitan Municipality (CoT) Supply Chain Management (SCM) division oversees and manages the procurement and purchasing function of the municipality. All tenders for services and goods are handled by this division. The CoT invites prospective suppliers to apply to be accredited and registered on its supplier database in compliance with the Preferential Procurement Policy Framework Act, 2000 Act No. 5 of 2000 (South Africa, 2000). The CoT does not do business with any suppliers that are not accredited and registered on the database” (*Supply Chain Management. Vendor Registration,* 2009).

1.2.1 Brief overview of the City of Tshwane procurement process

Clause 8.3 of the CoT SCM Policy Amendment Report (*SCM Policy Amendment Report,* 2011) approved on 27 September 2007, and amended on 24 February 2011, provides that the procurement of goods and services of the value of purchase (VAT inclusive) from:

- R0 up to R2000 should be procured through petty cash
- R2001 up to R10 000 should be procured through quotations
- R10 001 up to R30 000 should be procured through 1(one) formal written and 2 (two) other price quotations in accordance with council approved procurement framework
- R30 001 up to R200 000 should be procured through 3 (three) formal written price quotations and;
  - (i) Complying with the Municipal Finance Management Act (MFMA), 2003. Act No. 56 of 2003 (South Africa, 2003)
  - (ii) Sealed and placed in the box
  - (iii) Advertise for 7 (seven) days on notice board and website of municipality

(iv) Allocate in accordance with the point system

- Tender from above R200 001 up to 10 million and long term contracts.

  A competitive bidding process:

  (i) Advertised for at least 14 (fourteen) days on notice board and website of CoT municipality

  (ii) Advertised for at least 14 (fourteen) days in newspaper commonly circulating locally but not limited thereto

  (iii) Allocate in accordance with the point system

- Tender above 10 million.

  A competitive bidding process:

  (i) Advertised for at least 30 (thirty) days on notice board and website of Council; and

  (ii) Advertised for at least 30 (thirty) days in newspaper commonly circulating locally but not limited thereto

  (iii) Allocate in accordance with the preferential point system.

1.2.2 The mandate of the City of Tshwane Forensic Services Division

The CoT has, within its Group Audit and Risk (GAR) Department, a division identified as FS. FS is mandated by the Accounting Officer (City Manager) to investigate allegations of fraud, including procurement fraud, and corruption within the CoT (Anti-fraud and corruption implementation plan for the City of Tshwane, 2013:1). According to the MFMA (South Africa, 2003), the Accounting Officer has a duty to investigate and report financial misconduct; this duty has been duly delegated by establishing the FS business unit. According to the National Treasury Regulation 12.5.1 (South Africa. National Treasury, 2005), it is required that “criminal acts must be reported to the Accounting Officer and the South African Police Service (SAPS). This fiduciary duty is also one of the key responsibilities of FS”. The Prevention and Combating of Corrupt Activities Act, 2004 Act No. 12 of 2004 (South Africa, 2004), requires that corruption is reported and appropriate action is taken against offenders.

1.3 RESEARCH PROBLEM

Before research can be conducted on a specific topic, it is important for the researcher to know what the problem is, and the best way to solve the problem (Welman, Kruger & Mitchell, 2005:15).

The research problem identified for this study is as follows: Forensic investigators in the FS are unable to successfully deal with procurement fraud as a result of the lack of knowledge, skills and resources to conduct computer forensics during the investigation of procurement fraud. This research problem was confirmed by a CoT corruption and fraud risk assessment (Anti-fraud and corruption implementation plan for the City of Tshwane, 2013:11) conducted in 2012. This assessment found that the major challenge for forensic investigators attached to the FS is the lack of necessary computer skills and qualifications that would enable them to function effectively and carry out the mandate of the FS. Between the 2011/2012 and 2014/2015 financial years, 52 procurement fraud cases where registered; seventy percent of these were unsuccessfully investigated because of this problem.

During the 2011-2015 financial period, the CoT municipality lost 6.2 billion rand due to procurement fraud (City of Tshwane, Forensic Investigations. Internal Audit Reports, 2011-2015). According to the Anti-fraud and Corruption Implementation Plan for the City of Tshwane (2013), procurement fraud which resulted from supplier/service provider and employee collusion, was identified as a major problem within the CoT municipality. The impact thereof was major financial loss, which affects service delivery and causes adverse reputational damage to the CoT. According to the Reports of the Auditor-General South Africa to the Gauteng Provincial Legislature and Council on the City of Tshwane Metropolitan Municipality (2012), the CoT Forensic Audit section of the Internal Audit Division investigated and finalised 516 cases for the financial year 2011-2012. The nature of these cases covered a wide spectrum of activities including supply chain management, procurement fraud and financial misconduct.

According to the City of Tshwane, Forensic Investigations' Internal Audit Reports (2011-2015), seventy percent of procurement fraud cases investigated by CoT forensic investigators during the 2011-2015 financial period were unsuccessfully investigated; further, such cases were closed as suspects were undetected or the suspects who were charged were not successfully prosecuted. A total of twenty five percent of those cases were outsourced to a panel of external service providers, and suspects were successfully prosecuted as a result of the application of computer forensics. Five percent of those cases were transferred to the Special Investigating Unit (SIU) for further investigation. "The SIU is a public entity with powers of investigation and litigation. Its primary mandate is to recover and prevent financial losses to the state caused by acts of corruption, fraud and maladministration" (*Special Investigating Unit,* 2013).

1.3.1 Experience in the investigation of procurement fraud

The researcher is a former police officer, with four years of investigation experience in the SAPS's Organised Crime Unit. Furthermore, the researcher has six years' investigative experience in the GAR of the CoT, working as a senior forensic audit specialist at FS, and involved in the investigation of procurement fraud. The researcher was involved in the investigation of a number of procurement fraud cases. The researcher's experience will assist him in understanding the circumstances in which CoT forensic investigators need to conduct computer forensics during the investigation of procurement fraud.

From first-hand experience in his daily functioning as a CoT forensic investigator, preliminary discussions with forensic investigators at the CoT as well as a preliminary review of the relevant literature, the researcher confirmed that CoT forensic investigators lack the resources and skills required to successfully gather and analyse computer forensic evidence collected from computers used in the commission of procurement fraud. Thus, they are unable to effectively present evidence from data analysis that is admissible in court and in CoT's internal disciplinary proceedings.

Moreover, this problem is the result of a lack of training and the application of incorrect procedures when collecting computer forensic evidence, which results in evidence being disputed. There should be significant emphasis placed on research in the field of computer forensics, coupled with adequate training of CoT forensic investigators involved in this field. This study will attempt to highlight the value of computer forensics as a technique in the investigation of procurement fraud.

The researcher obtained a Bachelor’s Degree in Criminal Justice from the University of Venda in 2003, a Baccallaureus Technologiae (BTech) Degree in Forensic Investigation from the University of South Africa in 2012, and a certificate in the Prevention and Detection of Procurement and Contract Fraud from the University of Pretoria in 2013.

1.4 DELIMITATIONS OF THE STUDY

This study has the following delimitations:

1.4.1 Geographical Delimitation

This study is limited to the forensic investigators attached to the FS of the GAR within the CoT whose responsibility, amongst others, is the investigation of procurement fraud.

1.4.2 Time

This study focusses on procurement fraud cases, investigated by CoT forensic investigators during the 2011-2015 financial period, which were closed as suspects were undetected or cases were unsuccessfully prosecuted.

1.5 RESEARCH AIM

According to Oliver (2013:102), research aims are one of the most significant attributes of research. Oliver further states that research aims essentially express what you want to learn from the research being conducted.

The aim of this study was to explore the value of computer forensics in the investigation of procurement fraud among FS forensic investigators within the GAR at the CoT. The study concludes by making certain recommendations based on the findings of the research, which could be used to create an increased understanding and awareness of the value of computer forensics during the investigation of procurement fraud within the CoT.

1.6 PURPOSE OF THE RESEARCH

According to Denscombe (2002:25(a)), "there must be a reason for doing research otherwise there would be no point in spending time, money and effort undertaking the research." Denscombe (2002:25(a)) further declares that research purpose has to do with the focus of the research, and it provides the researcher with criteria to evaluate the results or outcome of the research.

The purpose of this research was:

- To explore the procedures that should be followed by CoT forensic investigators when conducting computer forensics during the investigation of procurement fraud.
- To discover new information on computer forensics during the investigation of procurement fraud, not previously known to the researcher, by exploring national and international literature, as well as existing practices thereof.
- To improve the CoT current procedure, within the confines of the legislative requirements.

- To arrive at recommendations for best practices, based on the results of the data analysis, that address the problem and enhance the investigative skills of CoT forensic investigators.
- To empower the researcher and CoT forensic investigators with new knowledge about computer forensics during the investigation of procurement fraud. This will contribute towards improving the quality of procurement fraud investigations presented before a court of law.

1.7 RESEARCH QUESTION

Research questions specify exactly what is to be investigated. They are things that are directly investigated by the researcher, specific things that are to be observed, measured, and interrogated in order to shed light on the topic (Denscombe, 2002:31(b)).

The following research questions are not only relevant but also essential to guiding this research as they provide key themes and shed light on the topic and research problem. For the purpose of this study, the researcher identified one primary research question:

- What is the value of computer forensics in the investigation of procurement fraud within the FS at the CoT?

Further to this, two secondary research questions were explored:

- What are the underlying reasons why forensic investigators within the FS in the CoT cannot optimally investigate procurement fraud?
- How can the efficiency of forensic investigators, in computer forensics, within the FS in the CoT be improved to successfully investigate incidents of procurement fraud?

1.8 KEY THEORETICAL CONCEPTS

The specification of conceptual definitions does two important things. Firstly, it serves as a specific working definition we present so that readers will understand exactly what we mean by a concept. Secondly, it focuses our observational strategy (Maxfield & Babbie, 2014:120).

The key theoretical concepts used in this study are:

1.8.1 Computer Forensics

Computer forensics is the process of applying scientific methods to collect and analyse data and information that can be used as evidence (Carrier, 2006:1). Similarly, Solomon, Barrett and Broom (2015:2) explain computer forensics as the process of identifying, preserving, analysing, and presenting evidence in a manner that is legally acceptable.

1.8.2 Forensic Investigation

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

1.8.3 Investigation of Crime

Investigation of crime is the systematic application of scientific methods and processes to the analysis of a crime committed (Becker & Dutelle, 2013:7).

1.8.4 Procurement Fraud

According to the National Fraud Authority (Annual Fraud Indicator) (2011:7), procurement fraud is a deliberate deception intended to influence any stage of the procure-to-pay lifecycle in order to make a financial gain or cause a loss. It can be perpetrated by contractors or sub-contractors external to the organisation, as well as staff within the organisation.

1.8.5 Computer Investigation

According to Carrier (2006:2), computer investigation is conducting computer analysis of a system suspected of containing evidence related to an incident or a crime.

1.9 VALUE OF THE RESEARCH

According to Welman and Kruger (2002:256), the value of research entails demonstrating a measure of research competence or problem-solving ability and, to a lesser degree, adding to the body of knowledge in a field of science. Denscombe (2002:43(b)) explains that the research must be relevant, in terms of contributing to existing knowledge, solving practical needs and it must be of relevance to current issues.

As a result, the results of this study strived to:

- Improve CoT forensic investigators' knowledge and competence regarding the application of computer forensics in the investigation of procurement fraud;
- Facilitate problem-solving with regard to CoT forensic investigators' inability to effectively investigate procurement fraud;
- Enhance CoT forensic investigators' investigative capacity through the facilitation of an improved procurement fraud prosecution rate;
- Contribute to the existing body of knowledge as an academic source for students and prospective researchers;

- Contribute to the broader South African community and the forensic investigation industry (with specific reference to those investigators responsible for investigating incidents of procurement fraud) since procurement fraud progressively remains to increase and negatively impact the South African economy.

1.10 RESEARCH DESIGN AND APPROACH

Research design is the programme that guides the investigator in the process of collecting, analysing and interpreting observation (Creswell, 2012:15). The researcher will conduct empirical research, since this study will involve going out into the field and ascertaining the personal experience and knowledge of the participants, as explained by Mouton (2001:149); that is, forensic investigators attached to the GAR of the CoT. According to Maxfield and Babbie (2014:4), experience and observation are key contributors of knowledge in empirical research. Maxfield and Babbie (2014:6), furthermore, describe empirical research as the production of knowledge based on experience or observation. Empirical research allowed the researcher to obtain information from the participants and had the advantage of allowing the researcher to probe participants' responses in much more detail during interviews.

The researcher gathered data by means of semi-structured interviews and a comprehensive literature study, which relates to a qualitative research approach. A qualitative approach entails conducting interviews with individuals or focus groups (Leedy & Ormrod, 2015:95). In addition to the review of the body of literature, semi-structured interviews were conducted with forensic investigators within the GAR of the CoT. The researcher used a qualitative research approach since, according to Creswell (2012:15), qualitative researchers study things in their natural setting, by going to the field, gathering information/data, analysing and arriving at findings, and making recommendations. Based on the writings of the abovementioned authors, the researcher considered the qualitative approach to be the best approach for this study.

1.11 POPULATION AND SAMPLING PROCEDURES

A target population or study population, according to Maxfield and Babbie (2014:186), consists of all the elements from which the sample is actually selected. A population can be described as the "totality of persons, events, organisation units, case records or other sampling units with which the research problem is concerned" (De Vos, Strydom, Fouché & Delport, 2007:199).

The ideal population for this research would have been all the forensic investigators in the South African municipality fraternity who apply computer forensics in the investigation of procurement fraud. It was, however, impractical to consult with this wide population; therefore, the researcher made use of a target population.

The target population for this study included forensic investigators attached to the GAR at the CoT municipality who investigate incidents of procurement fraud. The GAR comprises of three divisions: the Internal Audit Division, FS and Enterprise Risk Management Division.

Section 165(2) of the Municipal Finance Management Act (MFMA) (South Africa, 2003) requires that the internal audit unit of a municipality or municipal entity must, among other responsibilities, advise the Accounting Officer and report to the Audit and Performance Committee on the implementation of the internal audit plan and matters relating to internal auditing, internal controls, accounting procedures and practices, risk and risk management, and loss control. Section 62 (1) (c) (ii) of the MFMA (Act No. 56 of 2003) requires that the Accounting Officer of a municipality must take all reasonable steps to ensure that the municipality has and maintains effective, efficient and transparent systems of financial, risk management and internal control. FS is mandated by the Accounting Officer to investigate allegations of fraud, including procurement fraud, and corruption within the CoT, as discussed in paragraph 1.2.2.

Enterprise Risk Management is a continuous, proactive and systematic process, implemented by CoT Municipality's Executive Authority, Mayoral committee (MayCo), Accounting Officer, management and other personnel, applied in strategic planning and across the CoT. It is designed to identify potential events that may affect the Municipality, and manage risks to be within its risk tolerance, so as to provide reasonable assurance regarding the achievement of Municipality objectives. Enterprise Risk Management forms part of management's core responsibilities and is an integral part of the internal processes of an institution. Risk management is as much about identifying opportunities as it is about avoiding or mitigating losses, such as procurement fraud. That is, while it enables the effect of identified risk to an activity to be mitigated or reduced, it also provides the climate for additional opportunities for the activity once risks have been adequately counteracted. Some of the risks have a negative impact on an entity and, if not adequately controlled, will prevent the CoT and its Entities from achieving its objectives, aims or vision (City of Tshwane. Enterprise Risk Management Strategy, 2012:5-6).

Sampling, according to Denscombe (2002:11(a)), refers to a small portion of the entire population. De Vos et al. (2007:194) are of the view that qualitative researchers look for individuals, groups and settings where the specific processes being studied are more likely to occur. In this study, the lack of knowledge, skills, resources and the non-utilisation of computer forensics in the investigation of procurement fraud among forensic investigators in the FS of the CoT municipality were studied. The sample for this research was purposively selected from the total number of 62 CoT forensic investigators, attached to the FS, who are responsible for investigating procurement fraud within the CoT municipality.

In sharing sentiments with De Vos et al. (2007:194), the researcher purposively selected participants through the use of non-probability sampling. Babbie (2016:166) is of the opinion that purposive sampling is used when the researcher selects a sample on the basis of knowledge of the population, its elements and the nature of the research aim. The researcher has extensive knowledge of the population and its elements since he is attached to the GAR division which forms the target population of this study. Purposive sampling was thus applied to select a sample of 25 FS forensic investigators who investigate incidents of procurement fraud within the CoT municipality. Data was gathered until saturation had been reached.

1.12 DATA COLLECTION

According to Denscombe (2010:70), it is crucial to gain access to documents and people for the purposes of research, or else researchers will engage in speculation on the subject. Mouton (2001:98-105) suggests that data collection methods in qualitative research include observation, interviewing and documentary sources.

The manner in which data is collected depends on the type of research and the purpose of the research. Since this study followed a qualitative approach, the researcher used a literature review and interviews as data collection techniques.

1.12.1 Literature Review

The researcher followed Mouton’s (2001:90) advice for the effective reading of literature, such as reading the most recent articles first, reading the abstract of an article before reading the whole article, and searching for articles which are relevant to the research topic. Once the researcher discovered that the literature or a source was relevant, he then read the book in detail. The researcher gathered information from relevant national and international journal articles, publications and other literature sources to assist in providing answers to the research question. This literature was sourced in respect of the various concepts mentioned below:

- Computer forensics
- Computer data analysis
- Procurement fraud.

1.12.2 Semi-structured interviews

The researcher conducted semi-structured interviews facilitated by means of an interview schedule as another method of collecting data, as outlined by Welman and Kruger (1999:166). One interview schedule was used and contained a collection of questions that were derived from the research problem, research question and research aim. This allowed the interviewees to provide open-ended answers in a comprehensive manner.

The researcher made use of a voice recorder to record the interviews. These recorded interviews were transcribed for the purpose of data analysis. Written consent was obtained from the research participants before commencing with the interviews.

The researcher followed the guidelines provided by Leedy and Ormrod (2015:147-149) when interviews were conducted:

- The researcher compiled an interview schedule containing questions regarding the research topic;
- Found a venue that was convenient and free from any disturbance;
- The interviews were conducted in a suitable location to ensure that interviewees were at ease;
- The researcher obtained prior written permission from the CoT municipality to conduct the interviews;
- The researcher only asked questions related to the research and recorded the answers exactly as they have been provided by the interviewees. The researcher has not, under any circumstances, attempted to alter what the interviewees have said nor put words in the interviewees' mouths. The researcher only listened to what the interviewee said and did not lead the interviewee;
- For the purposes of ensuring that confidentiality is maintained, the researcher only referred to the interviewees as participants.

Prior to commencing with the interviews, the researcher conducted a pilot study at the workplace using the interview schedule. During this pilot study, colleagues who did not form part of the sample, and who performed the same type of work as the study participants, were interviewed to identify possible shortcomings and any amendments needed to be made to the interview schedule, as suggested by Maxwell (2004:93).

1.13 DATA ANALYSIS

De Vos et al. (2007:333) define “Data Analysis” as a process of interpreting and giving order to a large volume of data. The viewpoints of all the respondents were compared; those with similar views were grouped together and those with different views were grouped together, and their responses analysed.

The researcher made use of the data analysis spiral, which is applicable to a wide variety of qualitative studies as explained by Leedy and Ormrod (2015:161). This spiral procedure entails using data to form the basis of research study by observing the following steps:

- Organising raw data – the researcher organised the data by breaking it into smaller pieces and created a computer database;
- Perusing data – the researcher needed to know what the data contains;
- Data classification and analysis – the researcher grouped the data into categories or groups and started with his analysis;
- Synthesizing the data – the researcher integrated and summarised the data; and presented the final report.

1.14 TRUSTWORTHINESS OF THE STUDY

Proposal developers need to convey the steps that they will take in their studies to check for the accuracy and credibility of their findings (Creswell, 2014:201). According to Creswell (2014:201), qualitative validity means that the researcher checks for the accuracy of the findings by employing certain procedures, while qualitative reliability indicates that the researcher's approach is consistent across different researchers.

According to Marshall and Rossman (2014:39), historically, concerns with the trustworthiness of qualitative research drew from the natural and experimental sciences for direction. Thus, reliability and validity – borrowed from more quantitative approaches – were the criteria against which the soundness of a qualitative study was judged. Lincoln and Guba (in Marshall & Rossman, 2014:40) came up with alternative constructs to capture qualitative validity and reliability, namely, credibility, dependability, confirmability, and transferability.

The following validation strategies, as suggested by Creswell (2014:201), were applied in this study:

- Triangulation

  The researcher triangulated different data sources by examining evidence from the sources and used it to build a cohort justification for themes.
- Member checking

  The researcher determined the accuracy of the qualitative findings through taking the final report back to participants to determine whether these participants felt that they were accurately recorded.
- Rich, thick description

  The researcher used a rich, thick description to convey the findings to participants by providing a detailed explanation of the research setting and the participants involved in the study.
- Clarifying bias the researcher brings to the study

  The researcher had from the onset of the study informed and commented on his occupational background and experiences in the field of this study as explained in the problem statement.

- Prolonged time in the field
  The researcher had continuously engaged with participants to build and maintain trust while conducting the research. The researcher developed increased experience with participants in their natural setting.

1.15 METHODS TAKEN TO ENSURE RELIABILITY

Reliability relates to the credibility of the findings of a particular study (Welman et al., 2005:145). O'Connor and Kleyner (2012:16) mention that the reliability programme must begin at the early stage or phase of a research project. This is the stage at which fundamental decisions are decided and will significantly affect reliability. If the research can be repeated elsewhere and reach similar research findings, then it can be said to be reliable.

The researcher conducted an in-depth literature review in order to gather reliable data. A thorough analysis of literature collected was done; the researcher ensured that the collected literature is considered reliable as it directly relates to the research topic. The literature that was used in this study was obtained from national and international textbooks and scientific journals related to the specific subject. The researcher made use of one interview schedule to interview all the participants in order to ensure that the same results were obtained, even if the research had to be repeated by another researcher. This further contributed to the reliability of the data collected from the interviews conducted.

1.16 ETHICAL CONSIDERATIONS

According to the University of South Africa (UNISA) *Policy on Research Ethics of the University of South Africa* (University of South Africa, 2007:7), researchers should respect and protect the dignity, privacy and confidentiality of participants. The researcher will adhere to UNISA's code of conduct for researchers.

Ethical guidelines serve as standards and the basis upon which each researcher ought to evaluate his/her own conduct, as described by De Vos et al. (2007:24).

The following ethical guidelines were adhered to during this study:

1.16.1 Protection from harm

The names of participants were not revealed so as to protect them from any unnecessary physical or psychological harm, thus, they were referred to as participants. The researcher also ensured that the necessary permission was obtained prior to conducting any interviews, and that the interviewees were provided with sufficient information on the research being conducted.

1.16.2 Informed consent

The researcher informed the participants, in advance, of the purpose and nature of the research; this allowed each participant to make an informed decision of whether to participate or not. Written consent was obtained from each participant. The CoT forensic investigators, who were selected as the sample of participants, agreed to be interviewed. The interviews were conducted at their convenience and at suitable venues chosen by the researcher. The researcher reported his findings honestly, based on the interviewees’ responses.

1.16.3 Acknowledgement of sources

All sources cited were duly acknowledged to ensure that no plagiarism was committed. Appropriate references to every author quoted in this study were made, and the researcher acknowledged the literature by including a comprehensive list of references at the end of the study.

1.16.4 Confidentiality

Confidentiality was guaranteed since the names of the participants remained anonymous. Interviews were conducted at the participants' work stations, privately and individually.

1.16.5 Right to privacy

The right to privacy of participants was respected and maintained. According to Leedy and Ormrod (2015:128), participants should not participate in research which could cause them embarrassment.

1.17 SUMMARY

This chapter introduced the research by providing a short background to study, after which an exploration of the research problem was presented. This was followed by an explanation of the research objectives and the research questions relevant to the study. This chapter further provided a brief overview of how data was collected and analysed. All the limitations applicable to the study, as well as all the problems encountered during the course of the study were outlined herein. All the relevant key terms were clarified, and the chapter concluded with a brief description of the method chosen to ensure the reliability and validity of the study, as well as a brief overview of the ethical framework within which the research was conducted.

CHAPTER TWO
THE APPLICATION OF COMPUTER FORENSICS IN FORENSIC INVESTIGATION

2.1 INTRODUCTION

The application of computer forensics implies that a computer specialist trained in computer forensics can examine a computer to find clues as to what happened. This role can only be performed by a computer forensics specialist. Solomon et al. (2015:2) and Vacca (2011:4) agree that computer forensics must only be conducted by trained computer specialists, otherwise the credibility of the evidence obtained during analysis will be in jeopardy.

If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined by anyone other than a trained and experienced computer forensics specialist or examiner, the usefulness and credibility of that evidence will be tainted and questionable, as also pointed out by Vacca (2011:4). Although the rules governing each activity can be dramatically different, the approach to computer forensics is roughly the same (Solomon et al. 2015:2).

This chapter provides an overview of the application of computer forensics in forensic investigation, including the concepts, tools and common activities that will prepare forensic investigators with a solid understanding of the field of computer forensics. This overview will be followed by a discussion of the methodology of computer forensics, types of computer forensic technologies and basic computer forensics tools and techniques. This chapter concludes by explaining the concept of computer examination and computer evidence analysis.

After reading this chapter, forensic investigators will have an improved understanding of the process of finding, recovering, collecting and analysing computer evidence. They will also gain insight into how to perform the most common tasks that forensic investigators encounter in an investigation. The information contained in this chapter will expand forensic investigators' knowledge and abilities in the application of computer investigations. Challenges related to the application of computer forensics, which are prevalent in the industry, are also highlighted herein.

A brief overview of various authors' understandings of the concept 'computer forensics' follows for discussion, in order to theoretically contextualize this concept.

2.2 BRIEF OVERVIEW OF THE CONCEPT 'COMPUTER FORENSICS'

Vacca (2011:4) defines computer forensics as the collection, preservation, analysis and presentation of computer-related evidence. Vacca (2011:4) further refers to computer forensics as computer forensic analysis, electronic evidence discovery, digital discovery, data discovery, data recovery and computer examination.

In support of Vacca (2011:4), Solomon et al. (2015:2) also define computer forensics as the process of identifying, preserving, analysing and presenting digital evidence in a manner that is acceptable in a legal proceeding. The computer forensics process requires a vast knowledge of computer hardware and software in order to avoid the accidental invalidation or destruction of evidence and to preserve evidence for later analysis. A computer forensics review involves the application of investigative and analytical techniques to acquire and protect potential legal evidence; therefore, a professional within this field needs to have a detailed understanding of the local, regional, national and international laws affecting the process of collection and retention of computer evidence. This is especially true in cases involving attacks that may be waged from a widely distributed system located in many separate regions.

Marcella and Greenfield (2002:18) share a similar view with Vacca (2011:4) and Solomon et al. (2015:2) in that they claim that computer forensics deals with the presentation, identification, extraction, and documentation of computer evidence. Marcella and Greenfield (2002:18) maintain that this field is relatively new to the private sector, but it has been the mainstay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s. Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results pertaining to computer evidence processing.

Kruse and Heiser (2002:2) are of the view that computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. It is often more of an art than a science, but as in any discipline, computer forensic specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual. It is unfortunate that computer forensics is sometimes misunderstood as being somehow different from other types of investigations. If one were investigating a murder that took place at Sammy Marks Square, for example, the forensic investigator would typically photograph the scene, look for evidence, and take samples of the crime scene, including control samples to compare to the evidence. The collection of evidence proceeds similarly in a computer investigation, however, a number of forensic investigators approach computer investigations differently to other investigations, be it a standalone Processing Computer (PC), a server with a terabyte Redundant Array of Independent Disks (RAID) system, or even an entire network. Nobody expects the prosecution to rebuild Sammy Marks Square in the courtroom, but that is often the expectation in a computer crime case. Admittedly, digital data can be highly volatile. Due to general unfamiliarity, not only with computers themselves, this field is highly challenging.

Newman (2007:4) and Kruse and Heiser (2002:2) express similar views in describing computer forensics as those activities associated with the identification and preservation of computer or electronic evidence in support of some official or legal action. Additionally, analytical and investigative techniques are used to examine this evidence and data that is magnetically stored or encoded using the binary number system.

Kruse and Heiser (2002:2) further emphasize that the basic methodology consists of the following:

- Acquire the evidence without altering or damaging the original;
- Authenticate that your recovered evidence is the same as the originally seized data;
- Analyse that data without modifying.

Nelson, Philips and Steuart (2010:02) suggest that computer forensics involves obtaining and analysing digital information for use as evidence in civil, criminal, or administrative cases. Computer forensics, as outlined by Nelson et al. (2010:02), involves scientifically examining and analysing data from computer storage media so that the data can be used as evidence in court.

According to the International Council of Electronic Commerce Consultants (better known as the EC-Council) (2010:03), computer forensics is “the preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found.”

From the aforementioned discussions, it is clear that authors define computer forensics similarly as a process of collection, preservation, analysis and presentation of computer-related evidence. However, the researcher established that even though computer forensics is complicated investigation, its methodology is not different from any other types of investigation.

A synopsis of factors that necessitate the application of computer forensics in forensic investigation follows for discussion.

2.3 THE NEED FOR COMPUTER FORENSICS

As enterprises become more complex and exchange more confidential information online, high-tech crimes are increasing at a rapid rate. It is not surprising that computer forensics has become essential to the corporate world, and law enforcement organisations or agencies (Solomon et al. 2015:1).

Nelson et al. (2015:2) are in agreement with Solomon et al. (2015:1), by explaining that, as the world becomes more of a playing field, with more people online who have access to the same information, the need to standardise computer forensics processes has become more urgent. Nelson et al. (2015:2) further suggest that the field of computer forensics can encompass items such as research and incident response. With incident response, most organisations are concerned with protecting their assets and containing the situation, not necessarily prosecuting or finding the person responsible. Research in computer forensics is also not concerned with prosecution or the validity of evidence.

Furthermore, the EC-Council (2010:03) indicates that the need for computer forensics has become more apparent with the exponential increase in the number of cybercrimes and litigations in which large organisations are involved.

According to the EC-Council, computer forensics offers the following benefits to any organisation:

- Ensures the overall integrity and continued existence of an organisation’s computer system and network infrastructure.
- Helps the organisation capture important information if their computer system or networks are compromised. It also helps prosecute the case, if the criminal is caught.
- Extracts, processes, and interprets the actual evidence in order to prove the attacker’s actions and the organisation’s innocence in court.
- Efficiently tracks down cyber criminals and terrorists from different parts of the world. Cyber criminals and terrorists that use the internet as a communication

medium can be tracked down and their plans known. IP addresses play a vital role in determining the geographical position of terrorists.

- Tracks complicated cases such as procurement fraud and e-mail spamming.

A computer forensic expert ensures that the following rules are upheld during an investigation, as confirmed by the EC-Council (2010:04):

- No possible evidence is damaged, destroyed, or compromised by the forensic procedure used to investigate the computer (preservation of evidence).
- No possible computer malware is introduced to the computer being investigated during the analysis process (prevention of contamination of evidence).
- Any extracted and possibly relevant evidence is properly handled and protected from mechanical or electromagnetic damage (extraction and preservation of evidence).
- A continuing chain of custody is established and maintained (accountability of evidence).
- Professional ethics and legality are maintained (ethics of investigation).

Shinder and Tittel (2002:02), in support of what was elevated by the EC-Council (2010:04), mention that universal digital accessibility opens up new opportunities for the unscrupulous. Millions of dollars and rands are lost to computer-savvy criminals by both businesses and consumers. Until recently, many Information Technology (IT) professionals and law enforcement officers lacked awareness of and interest in the cybercrime phenomenon and the tools needed to tackle this global problem. Finally, however, there was a certain amount of antipathy between the two most important players in an effective fight against cybercrime: law enforcement agencies and computer professionals, to control the cybercrime problem and to make computers and the internet much safer to use.

The researcher has observed that due to an increased number of problems caused by cybercrime, the need for computer forensics becomes apparent in order to mitigate and subsequently deal with computer crimes around the globe. Different law enforcement agencies must cooperate and work together in order to successfully fight cybercrime.

A summary highlighting the objectives of computer forensics follows for discussion.

2.4 OBJECTIVES OF COMPUTER FORENSICS

The overall objective of all computer forensic phases (preservation, identification, extraction, interpretation and documentation) is to detect a computer incident, identify the intruder, and prosecute the perpetrator in a court of law (International Council of Electronic Commerce Consultants, 2010:04)

The main objectives of computer forensics are summarised as follows:

- To recover, analyse, and preserve the computer and related materials in a manner that can be presented as evidence in a court of law.
- To identify the evidence in a short amount of time, estimate the potential impact of the malicious activity on the victim, and assess the intent and identity of the perpetrator.

This view is expressed by authors such as Reyes and Wiles (2007:3), who explain that the ultimate goal of computer forensics is to determine the nature and events concerning a crime and to locate the perpetrator by following a structured investigation procedure. Computer forensic investigators must apply the following two tests in order for evidence of computer forensics to survive in a court of law:

- **Authenticity** Where does the evidence come from?
- **Reliability** Is the evidence reliable and free of flaws?

Pachghare (2015:375) shares a similar view as that of the EC-Council (2010:04) in that he suggests that the main objectives of computer forensics is preservation of the data, identification of the data, extraction of the information, documentation of the evidence found and interpretation of the information that has been collected. The primary objective of computer forensics is the secure collection of data stored on the computer system. The proper analysis of the collected data, so as to prepare strong evidence about the crime, is the second objective of computer forensics.

The researcher therefore concludes, based on his own experience and information from reviewed studies, that the objectives of computer forensics are: preservation, identification, extraction or recovery, analyses and documentation of data. Appropriate implementation of the abovementioned objectives will lead to the successful presentation of computer evidence in the court of law and the subsequent prosecution of offenders.

The basic computer forensic methodologies that forensic investigators should apply during an investigation follow for discussion.

2.5 COMPUTER FORENSIC METHODOLOGIES

The EC-Council (2010:04) concisely explains that computer forensics tools and methodologies are major components of organisations' disaster recovery preparedness and play a decisive role in overcoming and tackling computer incidents. Due to the growing misuse of computers to conduct criminal activities, there must be a proper set of methodologies to use in an investigation. The evidence acquired from computers is fragile and can be easily erased or altered, and the seized computer forensics may differ depending on the procedures, resources, and target company.

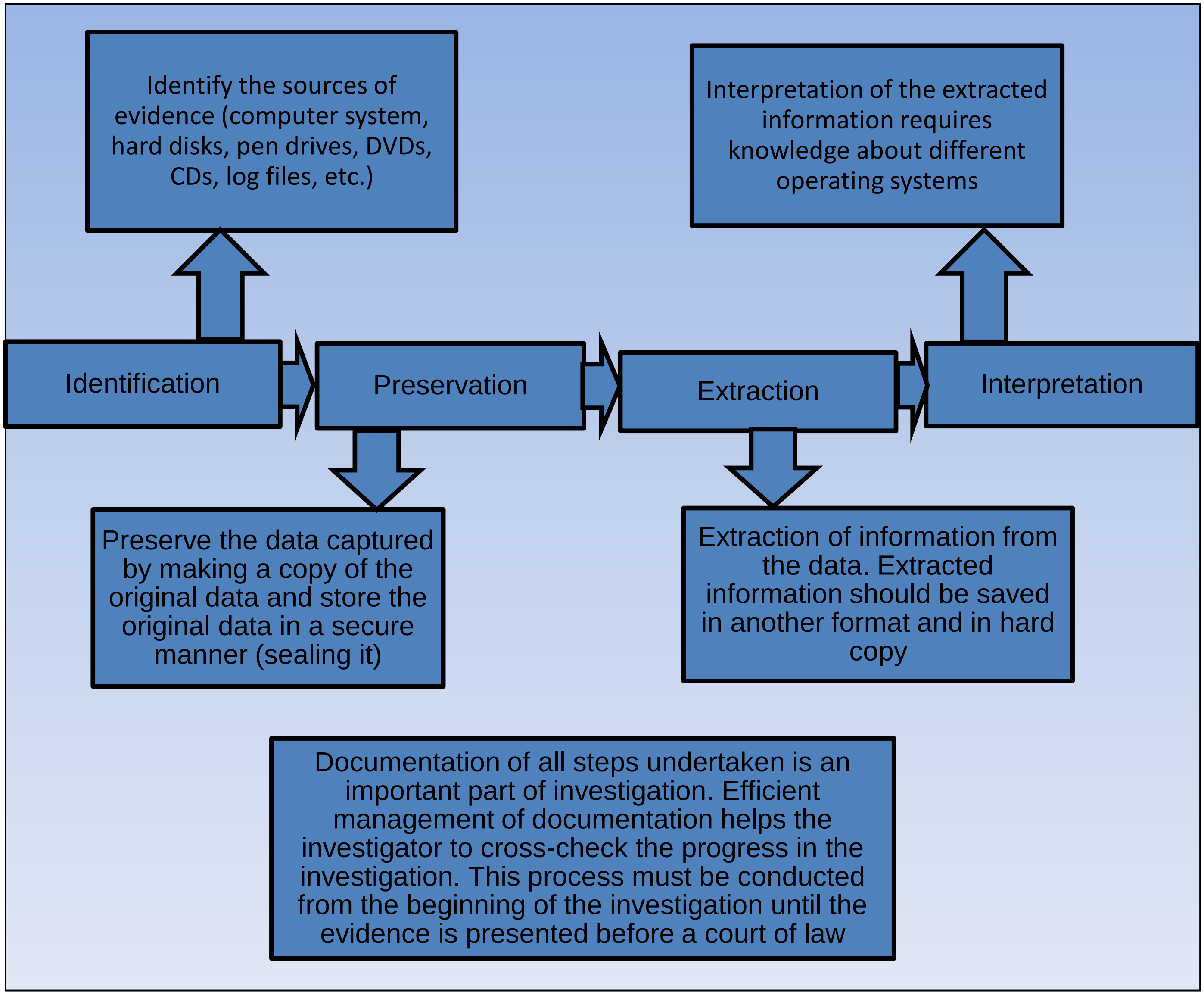
Computer forensic tools will enable the forensic examiner to recover deleted files, hidden files, and temporary data that the user may not locate. A forensic investigator must focus on fundamental areas such as standalone computers, workstations, servers, and online channels. The investigation of standalone computers, workstations, and other removable media can be simple. The examination of servers and online channels, however, can be complicated and tricky. During investigations, logs are often not examined or audited. The investigator must realise that logs play a key role during investigations; they must be given due importance, as they could provide a lead in the case. Computer forensic methodologies consist of the following basic activities, according to the EC-Council (2010:05):

- ***Preservation****:* the forensic investigator must preserve the integrity of the original evidence. The original evidence should not be modified or damaged. The forensic examiner must make an image or a copy of the original evidence and then perform the analysis on that image or copy. The examiner must also compare the copy with the original evidence to identify any modifications or damage.
- ***Identification****:* before starting the investigation, the forensic examiner must identify the evidence and its location. For example, evidence may be contained in hard disks, removable media, or log files. Every forensic examiner must understand the difference between actual evidence and evidence containers. Locating and identifying information and data is a challenge for the digital forensic investigator. Various examination processes, such as keyword searches, log file analyses, and system checks will help an investigation.
- ***Extraction****:* after identifying the evidence, the examiner must extract data from it. Since volatile data can be lost at any point, the forensic investigator must extract this data from the copy made from the original evidence. This extracted data must be compared with the original evidence and analysed.
- ***Interpretation****:* the most important role a forensic examiner plays during investigations is to interpret what he or she has actually found. The analysis and inspection of the evidence must be interpreted in a lucid manner.
- ***Documentation****:* from the beginning of the investigation until the end (when the evidence is presented before a court of law), forensic examiners must maintain documentation relating to the evidence. The documentation comprises the chain of custody form and documents relating to the evidence analysis.

Similar to what was stated by the EC-Council (2010:05), Pachghare (2015:376) explains the phases of computer forensic methodologies (see Figure 2.1 below) as follows:

- Identification
- Preservation
- Extraction
- Interpretation

Figure 2.1: Computer forensics methodology phases (figure developed by the researcher)


Identify the sources of evidence (computer system, hard disks, pen drives, DVDs, CDs, log files, etc.)
Interpretation of the extracted information requires knowledge about different operating systems
Identification
Preservation
Extraction
Interpretation
Preserve the data captured by making a copy of the original data and store the original data in a secure manner (sealing it)
Extraction of information from the data. Extracted information should be saved in another format and in hard copy
Documentation of all steps undertaken is an important part of investigation. Efficient management of documentation helps the investigator to cross-check the progress in the investigation. This process must be conducted from the beginning of the investigation until the evidence is presented before a court of law

As outlined in **Figure 2.1**, above, this explanation of computer forensics methodologies confirms the view of Marcella and Menendez (2010:7), who agrees with Pachghare

(2015:376) and the EC-Council (2010:05) by confirming that the process of computer forensics methodologies consists of the following steps:

- Identification-documentation
- Collection or extraction-documentation
- Preservation-documentation
- Interpretation or analysis-documentation
- Communication.

Marcella and Menendez (2010:7) further state that the preservation of the integrity of the collected electronic evidence is tightly coupled to ensuring that there is a solid documentation process. The documentation process should be designed to authenticate and substantiate each step taken to identify, collect (extract), preserve and interpret or analyse the electronic evidence, as well as each individual who may have in any way interacted with (handled) the electronic evidence. This was also illustrated and supported by Figure 2.1, above.

2.5.1 Chain of Custody

It is the submission of Girard (2015:21) that chain of custody refers to a written chronological record of each person who had an item of evidence in his or her possession. The prosecution must account for the evidence along every step of the way, from its discovery, to its collection, to its analysis, to its storage, to its transfer and throughout the entire process of court proceedings and appeals.

Barrow and Rufo (2014:145) define chain of custody as the witnessed, written record of all the individuals who maintained unbroken control over the items of evidence. Chain of custody establishes the proof that the items of evidence collected at the crime scene are the same evidence that is being presented in a court of law.

These views are supported by Sammons (2012:52) who contends that when a computer is taken in as evidence it makes many stops on its road to trial. It is collected, logged in at the lab, stored, checked out for analysis and checked back in for storage. Each of these stops must be noted, so as to track each and every time the evidence item changes hands or locations. Without this detailed account, the evidence will be deemed untrustworthy and inadmissible.

Barrow and Rufo (2014:145) maintain that all evidence collected at a crime scene should be tagged; if the item cannot be tagged, then it should marked with the following information:

- Description of item
- Case number
- Date of collection
- Location of collection
- Collector's name and identifier
- Brand name
- Any serial number or garment information.

The chain of custody is not completed when the evidence is collected (Barrow & Rufo, 2014:145). It is imperative that all contacts made with the evidence after collection are recorded with the following information:

- Who had contact with the evidence
- The date and time the evidence was handled
- The circumstances for the evidence being handled
- What changes, if any, were made to the evidence

The following are current CoT processes as stipulates on FS investigation operational methodology:

- Electronic devices seizure form must be completed in full.
- Every step and everyone who came into contact with evidence must be registered on the investigation diary of the project file.
- Chain of custody must be maintained until the report is submitted or testimony is provided in internal disciplinary proceedings or criminal court.

2.5.2 Locard Principle

According to Sammons (2012:7), the Locard principle entails that in the physical world, when a perpetrator enters or leaves a crime scene, they will leave something behind and take something with them. Registry keys and log files are examples of digital traces that suspects will always leave on the scene of computer crimes. The ability to detect and analyse these artefacts relies heavily on the technology at the investigator's disposal.

Barrow and Rufo (2014:146) suggest that even the most cautious criminal will leave or pick up traces of identifying material. They further state that what a person leaves on the scene of a crime is resilient and factual physical evidence that cannot be mistaken.

Vacca (2011:317) submits that the Locard principle implies that where there is a contact between two items, there will be an exchange and every contact will always leave a trace.

The views of these authors are also supported by the CoT FS investigation operational methodology, which maintains that the Locard principle refers to when two people meet, and/or a person and an object meet, there will always be clues transferred/left behind to reconstruct the crime and to identify the perpetrator. Therefore, when conducting an investigation all aspects related to the irregularity must be scrutinised.

The above discussion leads the researcher to conclude that documentation is the most crucial process in computer forensics methodology and shall be done after each and every step, from the beginning of the investigation until the presentation of the evidence before a court of law.

The four separate phases involved in computer forensics follows for discussion.

2.6 COMPUTER INVESTIGATIONS: A FOUR-STEP PROCESS

According to Maras (2015:34), there are four distinct steps in computer forensic investigations: acquisition, identification, evaluation and presentation.

2.6.1 Acquisition

The acquisition step involves the process of evidence retrieval in computer forensic investigations, from the search for the evidence to its collection and documentation (Maras, 2015:34).

Newman (2007:6) confirms that evidence must be preserved for court or corporate use. The documentation of every step must be developed. The first responder must ensure that all evidence is protected and documented. The chain of custody or chain of evidence begins at this point in time. This view is expressed by authors such as Kanellis, Kiountouzis, Kolokotronics and Martakos (2006:58) who, in their study, indicate that the investigator should know which tool to use in order to make the evidence apparent. It is important to identify and capture the evidence without losing its integrity and values so that it is admissible in court. According to Nelson et al. (2015:254), the first task in digital forensics investigation is to make a copy of the original drive. This procedure preserves the original drive to ensure that it does not become corrupt and damage the digital evidence.

2.6.2 Identification

According to Newman (2007:6), evidence is presented in both a physical and logical context. The physical context relates to the hardware or software components, such as a particular disk drive. The logical relationship might include the address or location of the evidence on a disk drive. Kanellis et al. (2006:59) point out that, to identify potential evidence, the investigator needs extensive knowledge of computer hardware and software, including operating systems, file systems, and cryptographic algorithms.

In addition to the identification step, from the researcher’s experience, an investigator should explain and document the origin of the evidence and its significance. Given that the evidence can be interpreted from a number of different perspectives, this phase determines the context in which the evidence was found. It looks at both the physical environment and the logical context of the location of electronic evidence. As suggested by Maras (2015:35), the identification stage also involves making evidence that was otherwise concealed visible to the forensic analyst for review in the next stage of the computer forensic process: evaluation.

2.6.3 Evaluation

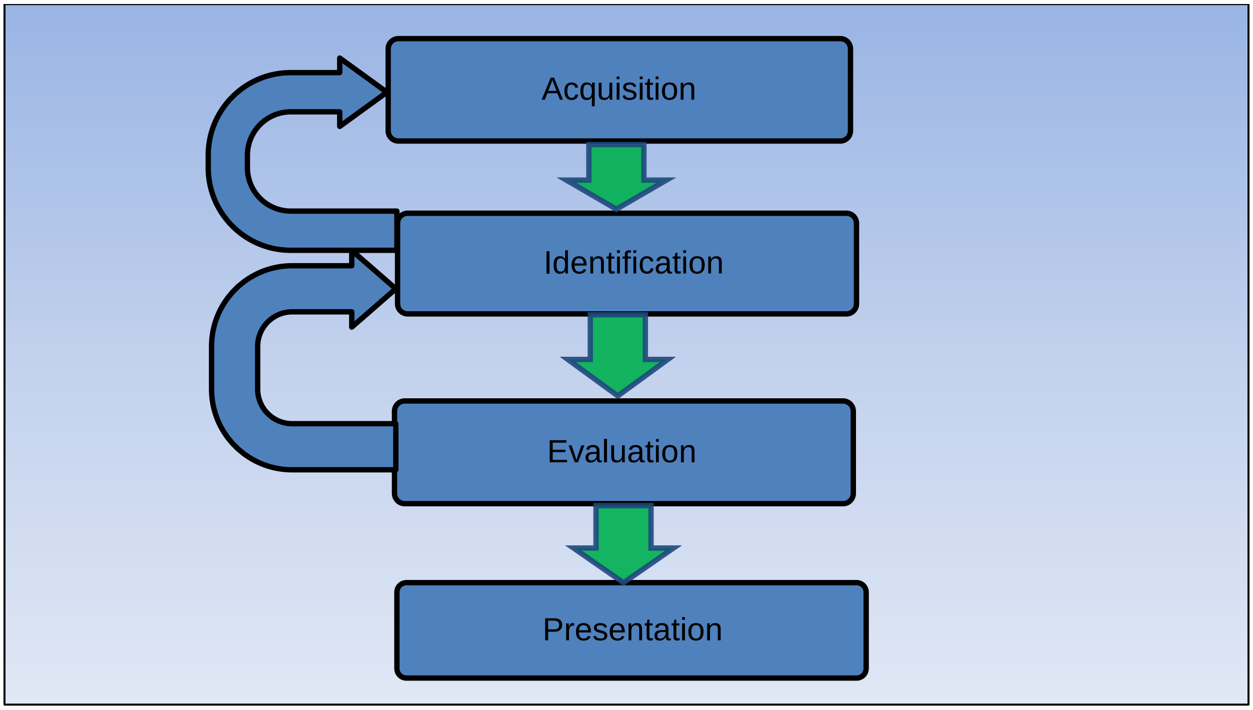
Maras (2015:37) suggests that, in the evaluation step of the computer forensics process, the data retrieved during investigation are analysed to establish their significance and relevance to the case at hand. The validity and reliability of the data are also examined. Only valid and reliable information that has been properly and lawfully documented, collected, processed, inventoried, packaged, transported, and analysed will be used for the next step in the computer forensic process: presentation. Newman (2007:7) concurs with Maras (2015:37) in stating that a computer forensic investigator in concert with a computer forensic examiner must determine the relevance and validity of the evidence collected by the first responder.

2.6.4 Presentation

Newman (2007:7) indicates that, during a formal presentation, the forensic team must determine the worthiness of the various pieces of evidence. Lack of knowledge on the part of any forensic participant will degrade the presentation in the other’s favor. Maras (2015:37) confirms that the final stage, involves reporting data pertinent to the case that was found during the investigation. The evaluation of evidence by outside parties may be expected in this stage. Accordingly, computer forensic investigators must be prepared to testify in court. During testimony, they are usually required to defend their personal qualifications, methods, validity of procedures, handling of evidence, and findings.

In their study, Kanellis et al. (2006:61) agree with Maras (2015:37) and Newman (2007:7) by emphasising that the presentation or generation of a forensic report of the results of an analysis is a crucial step in an investigation. Every step in the forensic analysis has to be carefully documented. The computer forensic examiner should be able to explain complex technological concepts in simple terms. The meaning and significance of the results obtained must be clearly conveyed. Notwithstanding the above discussions, Kanellis et al. (2006:61), Maras (2015:37) and Newman (2007:7) maintain that there are four distinct steps required in computer forensic investigations. As depicted in Figure 2.2, below, the first two steps repeat until the investigation is completed.

Figure 2.2: The four-step process of computer forensic investigation (figure developed by the researcher)



It is worth noting that, as perceived by the researcher and illustrated in **Figure 2.2**, above, in computer forensic cases validity and reliability of data will virtually be tested or disputed in a court of law. During the four-steps of investigation, a computer forensic examiner should properly and legally identify, preserve, collect, evaluate or analyse, document and present all the data in order to determine the validity and reliability of the evidence.

The different computer forensic technologies follow for discussion, that is, computer forensics and network forensics.

2.7 TYPES OF COMPUTER FORENSIC TECHNOLOGIES

Computer forensics and network forensics are two main types of computer forensic technologies. Computer forensics deal primarily with gathering evidence from computer media seized at the crime scene, whiles network forensics deal primarily with in-depth analysis of computer network evidence.

2.7.1 Computer Forensics

Computer forensics deals with the gathering of evidence from computer media seized at the scene of a crime. Principle concerns with computer forensics involve imaging storage media, recovering deleted files, searching slack and free space, and preserving the collected information for litigation purposes (Vacca, 2011:31). Several forensic tools are available to investigators in order to conduct computer forensics (Vacca, 2011:31). Tewari, Sastry and Ravikumar (2002:212) share a similar opinion with Vacca (2011:31) by suggesting that computer forensics deals with gathering evidence from computer media seized at the crime scene, by extracting hidden or deleted information from the computer disk. Furthermore, Tewari et al. (2002:211) state that special software tools and techniques are employed to analyse various levels of data storage and unearth the truth hidden in a maze of data. A skilled computer forensic expert can easily identify and prove the *modus operandi* of a perpetrator of a computer crime. It is also possible to analyse the habits of the user and prove the offence by making digital evidence speak against the offender.

In light of the above, and as indicated by Maras (2015:27), computer forensics concerns the process of obtaining, processing, analysing, and storing digital information for use as evidence in criminal, civil and administrative cases. This type of information can be obtained from computers and other electronic devices such as printers, scanners, copiers, compact discs (CDs), digital versatile discs (DVDs), Blu-ray discs, external hard drives, universal serial bus (USB) flash drives, magnetic tape data storage devices, cameras, mobile phones, fixed telephony, faxes, personal digital assistant (PDAs), portable media players (e.g., Apple's iPod) and gaming consoles (e.g., Microsoft Xbox). Data can be retrieved from existing files (even those that have been deleted, encrypted, or damaged) or by monitoring user activity in real time. The information acquired from computers and other electronic devices can be used as evidence of a wide range of traditional crimes, cybercrimes and computer misuses.

2.7.2 Network Forensics

According to the EC-Council (2010:2), network forensics is the capturing, recording, and analysis of network events in order to discover the source of security attacks. Capturing network traffic over a network is simple in theory, but relatively complex in practice. This is due to the large amount of data that flows through a network and the complex nature of internet protocol. Because recording network traffic involves a lot of resources, it is often not possible to record all of the data flowing through the network. An investigator needs to back up this recording data in order to free up recording media and preserve the data for future analysis.

Maras (2015: 270) defines network forensics as the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyse and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent. Maras (2015: 270) further mention that network forensics measure success of unauthorised activities meant to disrupt, corrupt, and/or compromise system components as well as providing information to assist in response to or recovery from these activities.

Furthermore, Vacca (2011:31) explains network forensics is a more technically challenging aspect of cyber forensics. It entails gathering digital evidence that is distributed across large-scale, complex networks. This evidence is often transient in nature and is not preserved within permanent storage media. Network forensics deals primarily with the in-depth analysis of computer network intrusion evidence. This discussion by Vacca (2011:31) is confirmed in the work of Grant and Shaw (2014:4) who explain that network forensics addresses volatile network artifacts. Just like random access memory (RAM) forensics, the data moving through the network across the wire or over the wireless frequency spectrum is dynamic and short-lived. While the lifespan of both RAM and network artifacts are short-lived, network artifacts are generally the much shorter lived of the two. Once the network packets containing the data have traversed the network, in order to perform any type of network forensic analysis on the packets, we have to first capture the packets from the physical medium and then analyse them.

Maras (2015:271) concurs with Vacca (2011:31) and with Grant and Shaw (2014:4) whose studies indicate that network forensics seeks to capture, analyse, and preserve network traffic. This traffic consists of packets, that is, units of data transmitted over the network. Each packet contains a header and a body. The header is located at the beginning of the packet and includes information on the source address, destination address, total number of packets, and specific packet's position within a sequence of packets. The body includes the content (data) that the packet is delivering. Moreover, Maras (2015: 271) mentions that network forensics also seeks to reconstruct events that have occurred and retrieve any potential evidence for later use in a criminal, civil, or administrative proceeding.

The researcher therefore concludes, based on his own experience and information established from reviewed studies, that network forensics is about monitoring and checking the network for any anomalies. This is done to detect and to determine the nature of the attack or intrusion within the legal framework of the company or organisation. Furthermore, it seeks to prevent any malicious or undesirable activities from occurring in the future.

Computer forensic duties that should be performed by computer forensics specialist follow for discussion.

2.8 DUTIES OF COMPUTER FORENSICS SPECIALIST

When perpetrators attempt to destroy incriminating computer data evidence, they leave behind vital clues. Computer data evidence is a reliable and essential form of evidence in computer forensics that should not be overlooked by computer forensics specialist. Computer forensics specialist should be able to successfully perform complex evidence recovery procedures with skill and expertise that lends credibility to a specific case (Vacca, 2011:6). In support of Vacca (2011:6), Champlain (2003: 267) states that computer forensics specialist can match an individual diskette to the PC used to save data on it. This type of information is especially useful in the case of suspects who have diskettes in their possession that can be associated with a PC located in their home or that of another suspected criminal. Currently diskettes are not used any more since they are outdated. Memory sticks and external hard drives, for example, are used in modern days.

Cornick (2014:163) is of the opinion that computer forensics specialist can reconstruct or recover previously deleted or destroyed information. Vacca (2011:6) mentions the following computer forensic services that should be performed by forensics specialist:

2.8.1 Data Seizure

Computer forensics expert must use their knowledge of data storage technologies to track down evidence.

2.8.2 Data Duplication/Preservation

The data seized must not be altered in any way. Computer forensics specialist should make exact duplicates of the needed data, and because they work on the duplicated data, the integrity of the original data is maintained.

2.8.3 Data Recovery

Using proprietary tools, computer forensics specialist should be able to safely recover and analyse inaccessible evidence. Their ability to recover lost evidence is made possible by the expert's advanced understanding of storage technologies.

2.8.4 Document Searches

Computer forensics specialist should be able to search over 100,000 electronic documents in minutes, rather than days. The speed and efficiency of these searches makes the discovery process less complicated and less intrusive to all parties involved.

2.8.5 Media Conversion

Some computer data are stored on old and unreadable devices. Computer forensics expert should extract the relevant data from these devices, convert it into readable formats, and place it onto new storage media for analysis.

2.8.6 Expert Witness Services

Computer forensics specialist should be able to explain complex technical processes in an easy to understand fashion. This should help judges understand how computer evidence was found, what it consists of, and how it is relevant to a specific case.

In support of Vacca (2011:6), Solomon, Rudolph, Tittel, Barrett and Broom (2011:217-225) list the following duties of computer forensics specialist:

2.8.7 Document everything, assume nothing

It is the primary duty of the computer forensics specialist to document everything carefully, consistently and neatly. Documentation will provide a good point of reference for jogging the memories of computer forensic investigators when the case is lengthy.

2.8.8 Interview and Diagrams

When one interviews a suspected computer criminal, create a list of who is interviewed, including their names, e-mail addresses, what they saw, when, where, and how they saw it. One might even end up with a confession. The use of diagrams is another method employed by computer forensics specialist to document and prove a case. Sometimes they use pictures or drawings to get their point across or to clear some uncertainties.

2.8.9 Collection and preservation of evidence

When gathering and preparing evidence, the computer forensics specialist should keep in mind that normal computer operations can destroy evidence in the memory, in the file slack, or in the swap file. When documenting physical evidence, such as hard disks and portable media, the original evidence should be placed in a sealed bag that cannot be unsealed without leaving a mark. The sealed bag should be clearly marked with the case information.

2.8.10 Analyse and validate evidence

Most computer forensics specialists use multiple software tools created by separate and independent software developers to analyse and validate results. By validating evidence, computer forensics specialists eliminate the likelihood of a successful challenge to the integrity of results based on the accuracy of the software tools used. Computer forensics expert should be able to refute claims that evidence was mishandled or that the tools used to analyse evidence were unacceptable.

2.8.11 Formulation of a forensic report

Computer forensics expert should, at the end of the investigation, prepare a report. The report should contain focused and specific information, as relevant to the case. It is worth noting, as perceived by the researcher and as is apparent from the information obtained from the literature reviews, that a computer forensic specialist can recover all or part of the deleted information from a computer. Likewise, electronic evidence can frequently be recovered by a forensic specialist from a hard drive that has been physically damaged by being dropped, fire damaged or water damaged. Furthermore, the ability of computer forensics specialist to frequently retrieve data, even after it has been destroyed, has heavily influenced the development of the law regarding preservation duties, reasonableness limitations on discoverability, and sanctions for spoliation.

The qualities of and training required by computer forensics investigators to efficiently investigate computer related investigations follows for discussion.

2.9 QUALITIES AND TRAINING OF COMPUTER FORENSICS INVESTIGATORS

Computer forensics investigators should have high level investigative experience and knowledge to conduct computer related investigations. These experts should be uniquely qualified to conduct investigations involving software piracy, data or information theft, computer crimes, misuse of computers by employees and any other technology issues (Vacca, 2011:12).

In support of Vacca (2011:12), Shinder and Tittel (2002:136) explain that a good computer forensics investigator should be an excellent observer who notices things, including the little things such as dates, names and places. Computer forensics investigators should have a very good memory to remember facts, names, places and dates. They should also be innately curious and always love to learn the facts of the case and about the people involved. Shinder and Tittel (2002:137) further indicate that, in addition to the above mentioned generic qualities, a computer forensics investigator should have a number of additional characteristics:

- A basic understanding of computer science: knowledge of how computers work (including both hardware and software).
- An understanding of computer networking protocols: how network intrusions and attacks work.
- Knowledge of computer jargon: unique vocational jargon.
- An understanding of hacker culture: should be an expert in hacker culture.
- Knowledge of computer and networking security issues: should be familiar with common security “holes”, security products (such as firewalls) and security policies and practices.

Solomon et al. (2011:13) similarly maintains that, to effectively fight computer crimes, everyone who deals with it must be educated. This includes the judges or presiding officers, prosecutors, law enforcement officers and all in IT communities. In light of these qualities and the required training of computer forensics experts, the researcher probes the following: Imagine what would happen to evidence if a law enforcement officer was not properly trained and, as a result of his/her actions, a good portion of evidence was destroyed. What would happen in a complex case if the prosecutor and the judge or presiding officer had little experience with computers? More likely than not, the accused would be acquitted of the crime. Before deciding what training a computer forensics investigator needs, one should evaluate what the role of such an investigator would be in computer forensics, as it is a very wide profession.

Solomon et al. (2011:13) list the following common roles that could involve the process of computer forensics:

- Law enforcement officials,
- Legal professionals,
- Corporate human resources professionals,
- Compliance professionals,
- Security consultants providing incident response services,
- System administrators performing incident responses,
- Private investigators.

Furthermore**,** Solomon et al. (2011:13) sustain that the position an individual holds in the criminal justice community dictates the type of training they require. For example, prosecutors should have training in electronic discovery and digital data, and on how to properly present computer evidence in a court of law. Detectives or computer specialists/investigators should have hands-on training in working with data discovery of all types and on various operating systems. They should know how to recover data, read log files, and decrypt data.

Computer forensics investigators should be trained in the proper use of various imaging utilities available to the computer examiner, knowledge of verification methodologies and the testing of forensic tools. They should understand the concepts, techniques and tools, and be provided with a solid foundation in concepts related to the investigation, preservation, and processing of computer-based evidence. Three specific technical training that are recommended are: hardware, software and procedural aspects

(Newman, 2007:130). Allen and Sawhney (2015:294) are of the opinion that, for computer forensic work, a computer science or accounting degree is more helpful than a criminal justice degree. Allen and Sawhney (2015:294) believe an accounting degree provides good background knowledge for investigating fraud through computer forensics. However, computer forensic investigators never stop training. They learn the latest methods of fraud detection, new software programs and operating systems by attending conferences offered by software venders and professional associations. Solomon et al. (2011:13) suggest that when law enforcement officials are originally trained at the academy, they should receive some type of basic training on computer crime and how to investigate such crimes. Ideally, all criminal justice professionals should receive training in computer crimes, investigations, computer network technologies, and forensic investigations.

From the views obtained through the literature review, and based on the researcher's experience, the researcher recommends that computer forensic investigators need at least a bachelor's degree in a related field, such as computer science, accounting or criminal justice, because computer forensics specialists need computer skills and investigative skills. Therefore, extensive training and education is required. Training never stops, as computer and electronic technology is changing so fast and improving daily.

Computer forensics investigators require a number of different tools to identify, retrieve, collect and analyse computer evidence. These tools follow for discussion.

2.10 BASIC COMPUTER FORENSIC TOOLS

Computer forensics investigator and security personnel should be acquainted with the basic techniques and tools necessary for a successful investigation of internet and computer-related crimes. Topics include: types of computer crime, cyber law basics, tracing e-mail to source, digital evidence acquisition, cracking passwords, monitoring computers remotely, tracking online activity, finding and recovering hidden and deleted data, locating stolen computers, creating traceable files, identifying software pirates, and so on (Vacca, 2011:47).

Solomon et al. (2011:163) list the following computer forensic tools to identify and acquire sufficient computer evidence:

- ***ByteBack***: data recovery and investigative tool that provides more functionality than just disk copying. Some of the features of Byte Back are cloning/imaging, automated file recovery, rebuilding partitions and boot records, media wipe, and media editor;
- ***dd***: dd utility copies and converts files;
- ***DriveSpy***: copies and examines drive contents;
- ***EnCase***: software programs used to analyse a computer for the collection of evidence. It can copy virtually any type of media, creating an identical image for analysis (static data support);
- ***FTK (Forensic Toolkit) Imager***: generates cyclic redundancy check (CRC) or message digest algorithm (MD5) hash values for disk-copy verification. It provides full searching capability for media and images created from other imaging programs;
- ***ProDiscover***: provides disk imaging and verification features. It provides the ability to create a bit stream copy of an entire suspect disk, including hardware protected areas, to keep the original evidence safe;
- ***SafeBack***: creates a bit stream image of hard disk drives and drive contents;
- ***SMART***: runs in Linux and provides a graphical view of devices in a system;
- ***WinHex***: supports recovery from lost or damaged files and general editing of disk contents.

In addition, Middleton (2005:17) lists and explains the following supplementary computer forensic tools for evidence collection and analysis:

- ***GetTime***: is used to document the time and date settings of a victim computer system by reading the system time and date from Complementary Metal-oxide semiconductor (CMOS). Compares the date/time from CMOS to the current time on your watch. This must be done before processing the computer for evidence;

- ***FileList, FileCnvt, and Excel©***: use *FileList* to catalog the contents of the disk. *FileCnvt* and *Excel* are used to properly read the output of the *FileList* program;
- ***Swap Files and GetSwap***: obtain data found in computer “Swap” or “page” files so that the data can later be analysed during an investigation. *GetSwap* will obtain such data from one or more hard drive partitions in a single pass; and
- ***GetSlack***: captures the data contained in the file slack of the hard drive. Then the created file will be placed on the Zip Drive.

The researcher therefore concludes, based on the information gathered from the reviewed studies, that a computer forensics investigator needs several different tools to identify, retrieve, collect and analyse computer evidence. As some of the evidence is hidden from the naked eye, it requires very specialised forensic tools in order to be accessed.

The various types of computer evidence follow for discussion.

2.11 TYPES OF COMPUTER EVIDENCE

For the successful prosecution of computer crimes, reliable and relevant computer evidence must be appropriately presented before a court of law. The following are types of computer evidence that can be collected and analysed to assist law enforcement agencies to successfully reduce computer crimes and to successfully prosecute those who are responsible for committing those crimes.

2.11.1 Electronic/Digital evidence

Electronic or digital evidence consists of any type of information that can be extracted from a computer system or other digital devices and that can be used to prove or disprove an offense or policy violation. Electronic evidence can be used to support a claim or can serve as an alibi. By analysing the evidence retrieved during computer forensic investigations, investigators attempt to figure out what happened, when it happened, how it happened, why it happened, and who was involved (Maras, 2015:38). Similarly, Casey (2011:7) defines electronic evidence as any data stored or transmitted using a computer, which supports or refutes a theory of how an offence occurred or that addresses critical elements of the offence such as intent or an alibi.

2.11.2 Physical/Real evidence

Maras (2015:40) explains that evidence collected from a computer investigation is not limited to what is extracted from computer hard drives and other electronic devices. Further, Maras (2015:40) comments that physical evidence found on computers and related electronic devices usually take the form of trace evidence and impression evidence. Printers, scanners, computer towers, external hard drives, CDs, DVDs and USB sticks are examples of physical evidence that must be taken into consideration during computer forensics investigations. This confirms the view of Solomon et al. (2011:53), who purport that a computer could be introduced as real evidence. If a suspect's fingerprints are found on the computer's keyboards, such real evidence could be offered as proof that the suspect used the computer. Sometimes real evidence that can conclusively relate to a suspect is called hard evidence.

2.11.3 Documentary evidence

Shinder and Tittel (2002:550) maintain that documentary evidence, related to computer forensics, usually refers to written documents that constitute evidence, for example, computer forensics analyst reports and expert opinion reports submitted before court. This view is supported by Solomon et al. (2011:55), who suggest that all evidence in written form, including computer-based file data, is called documentary evidence. Solomon et al. (2011:55) caution that all documentary evidence should be authenticated since anyone can create an arbitrary data file with desired contents. Therefore, the computer forensics investigator should prove that the evidence was collected appropriately and that the data it contains proves a fact.

2.11.4 Testimonial evidence

According to Solomon et al. (2011:53), a computer forensics investigator who testifies about the tests performed in the computer laboratory and the experts who seized and examined documents for digital evidence are actually providing testimonial evidence.

2.11.5 Demonstrative evidence

In their study, Shinder and Tittel (2002:550) point out that demonstrative evidence is when a computer forensics investigator or expert reconstructs the scene or incident of computer crime by using visual aids such a graphs, charts, drawings and models, and allows the court to view it. Solomon et al. (2011:57) concurs with Shinder and Tittel (2002:550) who state that demonstrative evidence consists of some type of visual aid.

It is best practice to look around the computer crime scene to identify all types of computer evidence before the collection and classification of such evidence. It is of utmost importance not to overlook any type of computer evidence as the value thereof will contribute to the positive presentation of the case before a court of law.

The recovery or retrieval of computer evidence follows for discussion.

2.12 COMPUTER EVIDENCE RECOVERY/RETRIEVAL

Bainbridge (2008:491) emphasises that it is important that the information or data (evidence) retrieved from the equipment is retrieved in such a way that its authenticity and veracity cannot be challenged. Forensic investigators or auditors need to appreciate the fact that a computer may be set up to erase data when switched off or re-booted. Bainbridge (2008:491) further cautions that a computer that is found switched on must not be turned off until the whole contents can be imaged, if possible. If the computer under suspicion of containing evidence is not switched on, it can only be switched on after getting expert advice. It may be desirable to remove and duplicate the hard disk. Specialist help and software may be needed to recover files that have been deleted. It is advisable to engage a computer expert who can give appropriate advice and guidance as to how information or data can be retrieved in its entirety without corruption or modification, so that challenges to its authenticity and integrity can be countered.

In support of Bainbridge (2008:491), Vacca (2011:14) maintains that the computer forensics specialist should take several careful steps to identify and attempt to retrieve possible evidence that may exist on a suspect’s computer system. According to Vacca (2011:14), the following steps should be taken:

- Protect the computer system from any possible alteration, damage, data corruption, or virus introduction.
- Discover all files on the computer system. This includes existing normal files that have been deleted, remaining files, hidden files, password-protected files, and encrypted files.
- Recover all (or as much as possible) of discovered deleted files.
- Reveal (to the greatest extent possible) the contents of hidden files as well as temporary or swap files used by both the application programs and the operating system.
- Access (if possible and legally appropriate) the contents of protected or encrypted files.

Holt, Bossler and Seigfried-Spellar (2015:333) emphasise that computer forensics specialist should document how the computer evidence was retrieved from the digital sources and how the digital evidence was seized. It is important for the computer forensics investigator to maintain detailed notes and documentation of the search and seizure process of the digital forensic investigation.

Computer evidence retrieval or recovery can only be conducted by computer forensics specialist or expert to prevent any alteration or damage to evidence. It is also paramount to take notes and document every step of evidence retrieval or recovery.

The significance of the computer evidence collection process, and the preservation of such evidence, follow for discussion.

2.13 COMPUTER EVIDENCE COLLECTION AND PRESERVATION

Vacca (2011:67) is of the view that one of the most crucial points of a case perhaps lies hidden in a computer in front of the investigator. The digital evidence collection process allows the investigator not only to locate key evidence, but also maintains the integrity and reliability of that evidence. Vacca (2011:67) emphasises that timing is of the essence during the digital evidence collection process.

Brown (2010:8) is of the view that the methods used for the collection of computer evidence can be one of the most highly scrutinised areas of the computer forensics process. It is essential that investigators use tested and proven collection methodologies. The collection phase of computer forensics is when artifacts considered to be of evidentiary value are identified and collected. Normally, these artifacts are digital data in the form of disk drives, flash memory drives, or other forms of digital media and data; however, they can include supporting artifacts such as corporate security policies, operating manuals, and backup procedures.

Hausman, Barrett and Weiss (2003:258) share a similar view with Brown (2010:8) in that they outline that forensic software is available for collecting data properly. Forensic software allows the computer forensic investigator to collect and digitally sign a container that electronically stores evidence. After evidence is placed inside a digital evidence bag, it is signed with a certificate to prove that no tampering has occurred since it was collected. Brown (2010:8) further explains that another form of collecting data involves the imaging of the system or system being compromised. This can be done by copying the entire drive at the binary level, or the data can be copied into a digital evidence bag. After a complete copy is made, it should be sealed as "read-only". After the complete copy of the data is collected and stored, it should be secured from tampering or alteration.

In his study, Vacca (2011:67) lists a number of helpful guidelines that the computer forensics investigator can follow to help preserve the data for future computer forensics examination:

a) Do not turn on or attempt to examine the suspect computer. This could result in the destruction of evidence.

b) Identify all devices that may contain evidence. Devices such as the following:
   - Workstation computers
   - Off-site computers (laptops, notebooks, home computers, senders and recipients of e-mail, and PDAs, etc.).
   - Removable storage devices (zips, jaz, Orb, floppy diskettes, CDs, memory sticks, smart media, compact flash, Optical Disk, SyQuest, Bernoulli, Microdrive, Pocketdrives, USB disks, and firewire disks, etc.).
   - Network storage devices (RAIDs, servers, sans, nas, spanned, remote network hard drives, back-tapes, etc.).

c) Quarantine all in-house computers:
   - Do not permit anyone to use the computers
   - Secure all removable media
   - Turn off the computers
   - Disconnect the computers from the network
   - Consider the need for court orders to preserve and secure the digital evidence on third party computers and storage media.

The preservation phase of computer forensics, according to Brown (2010:8), focuses on the preservation of artifacts in a way that is reliable, complete, accurate, and verifiable. In addition, Hausman et al. (2003:256) maintain that after the evidence has been identified, it must be properly collected and preserved so as to be used in court. If the evidence is not preserved properly, it may be inadmissible. The computer forensics process is built around the fact that computer evidence can be altered, lost, or destroyed. Preserving evidence is difficult in computers because the data itself is not physical; instead, it resides on physical devices. Furthermore, any affected system should be immediately imaged before any other investigative tools are used. This is to ensure that data is preserved in its current state or form.

Stephenson and Gilbert (2013:128) suggest that there are two major risks in collecting computer forensics data: loss and alteration. If the investigator is not careful, he can overwrite important data, thus losing it completely. Alternatively, he could overwrite part of it, thereby changing its meaning or erasing critical pieces, such as characters in passwords. Computer forensics data that was not handled appropriately will attract significant rebuttal in court. The bottom line is that the proper collection of computer forensics evidence is critical.

The researcher therefore concludes, based on the information from reviewed studies, that computer evidence is admissible if it can be proven with facts that it was collected and preserved under defined procedures and as part of routine organisational practices. These procedures must be established before the incident and collection of evidence occurs in order for the evidence to be admissible.

The analysis of computer forensics evidence follows for discussion.

2.14 COMPUTER FORENSICS EVIDENCE ANALYSIS

According to Solomon et al. (2011:2), computer forensics entails the critical analysis of a computer hard disk drive after an intrusion or crime. This is mainly because specialised software tools and procedures are required to analyse the various areas where computer data is stored. This often involves retrieving deleted data from hard drives and servers that have been seized by law enforcement. Solomon et al. (2011:2) explain that, during the course of forensic work, a computer forensics investigator will run into a practice that is called “electronic discovery”*.* Items in electronic discovery include data that is created or stored on a computer, computer network, or other storage media.

Examples of electronic discovery are:

- E-mail
- Word-processing documents
- Plaintext files
- Database files
- Spreadsheets
- Digital art or photos
- Presentations.

Electronic discovery using computer forensics techniques, according to Solomon et al. (2011:2), requires in-depth computer knowledge and the ability to logically dissect a computer system or network in order to locate the desired evidence. It may also require expert witness testimony to explain the exact method or methods by which the evidence was obtained and analysed to the court. Computer forensics has become a popular topic in computer security circles and in the legal community. Even though it is a fascinating field, due to the nature of computers, far more information is available than there is time to analyse. A key skill is to know when to stop looking for evidence; however, this is a skill that comes with time and experience.

In light of the above, and as indicated by Wilding (1997:111), the most revealing source of information in an investigation turns out to be the suspect’s personal computer, be it a standalone, network PC, or laptop. Time and time again, fraudsters and other criminals will be fastidious in destroying paper evidence while failing to realise the significance of the computer data. This may be explained by the fact that data stored in electronic from is seemingly invisible and only becomes intelligible once the computer comes to life. The examination of computer records can be overtly undertaken*,* where the suspected person or company is aware that an investigation of specified items is occurring.

Alternatively, the examination may be covert, whereby the client requests a search be undertaken of a computer in use by an employee suspected of committing fraud, or another misdemeanour, in such a way that the suspect remains unaware that the search has occurred. The reason for a covert search may be one of diplomacy: if evidence is found, disciplinary or legal action can be taken; if not, the employee, unaware that a search has been made, is not unduly upset or offended. Whatever the circumstances, the process of recovering computer data as potential evidence demands discipline, and requires a methodical and logical approach. Any examination of computers must be conducted lawfully. If there is any doubt as to the legality of accessing a computer, no further investigation should proceed until the issue is resolved.

Vacca (2011:14) suggested that computer forensics investigator should analyse all possibly relevant data found in special (and typically inaccessible) areas of a computer disk. This includes, but is not limited to, what is called unallocated space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as slack space in a file (the remnant area at the end of a file in the last assigned disk cluster, that is unused current file data but, once again, may be a possible site for obviously created and relevant evidence). Furthermore, Vacca (2011:14) indicates that a print out of the overall analysis of the computer system, as well as a listing of all possibly relevant files and discovered file data must be made.

In support of the above authors, and from the researcher's experience, a computer, or any other electronic data processing system or data storage device that has been identified as relevant to an investigation or is implicated in an offence, should always be subjected to a forensic analysis by a qualified computer examiner.

A presentation and discussion of various computer forensics evidence analysis processes follows.

2.14.1 Computer memories and network

The data that will be used for visual analysis consists of network forensic data describing Internet Protocol (IP) sessions. This data can consist of, but is not limited to, a time, date, IP address pair, session type, and duration. Session type identifies the communication event type (Vacca, 2011:221).

According to Wilding (1997:112), it is important to distinguish between volatile and non-volatile memory. Volatile memory on a PC is usually referred to as RAM. Data is held in RAM only when the PC is actively processing, that is, when the machine is switched on. As soon as the computer is switched off, the information in RAM disappears. Due to its impermanent nature, RAM is sometimes referred to as *transient, temporary or volatile memory.* Non-volatile memory usually refers to a disk which stores data, even when the computer is switched off. Typically, this storage medium is magnetic, as is the case with hard disks and diskettes. Increasingly, however, the storage medium may be optical and includes peripheral devices such as Write Once Read Many (WORM) drives, Compact Disk-Read Only Memory (CD-ROM) and even re-writeable optical disks. Wilding (1997:112) further explains that the user may elect to actively save his work to disk, or the software he is using may “auto save” information to disk while it is operating in RAM. Microsoft Windows, and applications written for Windows, often saves information to disk without the user’s consent or even knowledge. This phenomenon has proved helpful when retrieving information which would otherwise have been lost as soon as the suspect switched his computer off.

Wilding’s (1997:112) view is supported by Wiles (2007:57) who states that network trace evidence analysis is an ongoing process of the investigation, as the investigator tracks the attackers from one entity to another. Wiles (2007:57) cautions that computer evidence analysis can be complicated due to the sheer volume of data, but the use of a visualisation tool, such as Analyst’s Notebook, can simplify the process. Wilding (1997:112) further states that another form of memory is CMOS. CMOS chips have very low energy consumption and are used to store semi-permanent information about a computer’s parameters. Time, date, hard and floppy disk drive types, primary display (video graphics array (VGA) or super video graphic array (SVGA)), base and extend memory, system boot sequence and password checking are just some of parameters stored in CMOS. This parameter may have evidential value and it is therefore preferable not to alter CMOS information. Obviously, it may be impossible to access the computer without writing to CMOS, for instance where the system boot sequence has to be altered in order that the target PC may be booted from a system diskette. CMOS time and date are of particular importance as this parameter may vary from the real time and date; this will obviously affect the date and time-stamps allocated to files on the target computer. It is also possible to “sink” CMOS memory so that a PC “forgets” its parameter. This is usually achieved by removing the battery pack which feeds current to CMOS or the “jumper” which closes the electrical circuit that feeds it current. “Sinking” the CMOS data may be necessary in order to gain access to the disk, in the event that the computer is password protected.

Wilding (1997:113) further maintains that evidence processed in RAM, as in this instance, was likely written to a disk at some stage. However, even where a process has ended, as would be the case when the user had finished using a word processor, remnants of his work will be retained in memory and may be located there using text or string search methods. It is possible to search a text string in RAM and to view the contents using a debugging process. The volatility of RAM means that potential evidence is likely to be destroyed even as the examination is being undertaken. Therefore, examining RAM, even in the very rare circumstances where such a tactic is warranted, is a haphazard task. As can be seen, evidential information may be obtained from CMOS, RAM, magnetic or optical media. While the investigator needs to be aware of the basic functions and characteristics of three different types of computer memory, in practice the investigator needs to be intimately acquainted with just one of them. Forensic efforts usually concentrate on the examination of *non-volatile memory*, usually in the form of magnetic or optical disks. Evidence may also reside on backup media such as Digital Audio Tapes (DAT) and tape-streamers. It is always important, therefore, to include backup devices and tapes when reviewing a potential source of evidence or intelligence.

2.14.2 Computer Media Handling

It is recommended that lawyers, investigators, auditors and other professionals, who are likely to encounter potential computer evidence, acquaint themselves with the basics of handling computer media during the evidence analysis phase. Magnetic media is sensitive to heat and strong sunlight, strong magnetic fields, dirt and dust contamination; in addition, the substrate can be damaged by fingerprints and foreign objects. Sugary coffee can prove ruinous when spilled over floppy disks. Other mishaps include diskettes jammed into briefcases and damaged; paperclips and other objects stuck into disk drives; and backup tapes left on central heating radiators overnight (Wilding, 1997:114-115).

2.14.3 Password and Encryption

Johnson (2005:105) is of the view that encryption is a process of scrambling information so that it is not recognizable without descrambling it. It can also be used for authenticating information and verifying that information is correct. Password and encryption are difficult obstacles for the computer crime investigator to overcome if he/she is not prepared for them. Password crackers and cryptanalysis utilities that employ a variety of algorithms to gain access to the system, or encrypted information, are commercially available.

Encrypted files and password protected software packages have occasionally proved difficult to crack. Experience has shown that even where encryption and secure erasure is available it is generally under-used and that people usually ignore the basic principles of computer security. It is recommended that investigators make use of a password modification program called Novell NetWare Password Recovery (NTPASS) which enables total access to Novell NetWare file servers in the event that a suspect password is unknown. The software is designed to recover the password of up to 36 characters in length, regardless of the use of control character, or alpha-numerical combinations (Wilding, 1997:118). Another program mentioned by Wilding (1997:118), which can be profitable to investigators, is Access Data's password recovery program for Microsoft Word (WDPASS). When a file is analysed using WDPASS, the password is ascertained in a time of approximately one minute per protected file.

According to Solomon et al. (2011:162), the investigator will usually recognise an encrypted file when they attempt to open it with a known extension and it fails. Another sign of encrypted files is a collection of meaningless filenames.

Furthermore, Solomon et al. (2011:172) list the utilities to decrypt files:

- Zip Password by LastBit: password recovery utility.
- Passware Password Recovery Software: recover password from Microsoft (MS)-Office application file.
- ElcomSoft password recovery software: recover passwords from various application files.

The significance of the documentation of the forensic process during the handling, processing and preservation stages of computer forensics follows for discussion.

2.15 COMPUTER FORENSICS DOCUMENTATION

According to Casey (2011:470), documentation is essential at all stages of handling and processing digital evidence. The primary goal of documentation at the survey and preservation stages is to establish the authenticity of the evidence. Documenting who collected and handled evidence at a given time is required to maintain the chain of custody. Carefully and consistently, notes should be made of when the evidence was collected, from where, and by whom. Most importantly, documentation showing evidence in its original state is regularly used to demonstrate that it is authentic and unaltered.

Vacca (2011:82) further emphasises the significance of documenting the computer forensics process by stating that the documentation of forensic-processing methodologies and findings is important. This is even true concerning computer security risk assessments, computer incident responses, and internal audits; without proper documentation it is difficult to present findings in court or to others. If the computer security or internal audit finding becomes the object of a lawsuit, or a criminal investigation, then accurate documentation becomes even more important. The investigators should be taught a computer-evidence-processing methodology that facilitates good evidence-processing documentation and solid evidence chain of custody procedures. The benefits will be obvious to investigators, internal auditors and computer security specialists.

Newman (2007:187) concurs with Vacca (2011:82) and Casey (2011:470), and mentions that the name of the computer forensics “game” is documentation, documentation, and more documentation. Documentation creates a permanent historical record that must stand up to intense scrutiny and possible litigation. Documentation is an ongoing requirement throughout any incident scene investigation. Issues relating to electronic and computer evidence handling include documentation, labeling, packaging, transportation, and storage.

It is apparent, from the information obtained during the literature review, that a case can take more than a year to develop; thus, the more comprehensive the forensics investigator’s notes, the easier it is to provide accurate and less refutable testimony.

The forensic investigation report forms an integral part of the computer forensics investigation process and follows for discussion.

2.16 FORMULATION OF COMPUTER FORENSICS INVESTIGATION REPORT

Solomon et al. (2011:226) emphasise that a typical report format consists of several independent sections presented in the following order:

- Executive summary: brief explanation of the circumstances that required the investigation and a short detail of the significant findings.
- Objectives: this section states the specific purpose of the investigation.
- Analysis: this section provides a description of the evidence and steps taken to process that evidence.
- Findings: includes specific information listed in order of importance or relevance. This can include data and graphic image analysis, internet related evidence, and techniques used to hide data.
- Supporting documentation: this section includes how the investigator arrived at the findings in the previous section.
- Glossary: this section helps the reader understand the technical terms contained in the report.

According to Purpura (2013:298), a typical standard computer forensics report begins with a heading that includes the type of incident, date, time, and location. The next section consists of a list of persons involved in the incident along with their addresses, telephone numbers, ages, and occupations. Another section can include a list of evidence. The end of the report contains the name of the investigator and the status of the investigation. Diagrams and photographs may be attached. Vacca (2011:14) concurs with Solomon et al. (2011:226) and Purpura (2013:298) by providing a detailed list of which aspects should be included in the forensic report. Vacca (2011:14) explains that the report should provide an opinion on the following: the system layout; the file structures discovered; any discovered data and authorship information; any attempts to hide, delete, protect and encrypt information; and anything else that has been discovered and appears to be relevant to the overall computer system examination.

The above discussion leads to the conclusion that the investigator should stick to the point in easy to understand language. An impressive vocabulary is not an asset to a report. Comprehensiveness, neatness and good grammar are important factors that a forensic investigator should keep in mind when formulating a report.

2.17 SUMMARY

In this chapter, it has been established that computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. Four distinct steps in computer forensics investigations are acquisition, identification, evaluation and presentation. The methodology of computer forensics consists of the following steps: identification, collection or extraction, preservation, interpretation or analysis, documentation and communication. Thorough documentation must be undertaken for each and every step of the forensics investigation.

It has also been established that, when a computer-related crime has been committed, the computer evidence needs to be identified. The next step will be for information or data (evidence) to be retrieved. During the collection of computer evidence, it is essential that investigators use tested and proven collection methodologies. Computer forensics entails the critical analysis of computer evidence. This is mainly done by using the specialised software tools and procedures required to analyse the various areas where computer data is stored. Documentation is essential at all stages of handling and processing digital evidence. The goal of documentation is to establish the authenticity of the evidence, and its admissibility.

In Chapter Three, an overview of the investigation of procurement fraud is presented and discussed.

CHAPTER THREE
AN OVERVIEW OF THE INVESTIGATION OF PROCUREMENT FRAUD

3.1 INTRODUCTION

According to Katz (2012:1), SCM operations and procurement functions are highly susceptible to fraud due to their nature, as they are more complex in today's global environment. An organisation can fall victim to fraudulent activities at every step in its supply chain, both internally and externally, and through internal-external collusions. The failure to detect and reduce procurement fraud at the source can lead to large financial losses as the fraud manifests itself through supply chain processes. Good governance demands a thorough risk analysis, which includes an organisation's susceptibility to fraud. Supply chain fraud detection and reduction requires a new examination of an organisation's activities beyond starting at the end, i.e. the financial statements. Minor fraudulent activity can turn into a larger one, leading to a hard impact, as the fraudster gains more confidence with increasing non-detection.

Katz (2012:7) further highlights that the detection and reduction of procurement fraud, especially for a national or global supply chain, is a multi-dimensional problem that requires expertise in multiple disciplines in order to be resolved. It is not just one viewpoint to a problem, but multiple perspectives in parallel. Nigel and Samociuk (2006:1) indicate that procurement fraud and corruption are arguably the greatest unmanaged commercial risks of all time. This begs the question, are management and executives taking procurement fraud and corruption seriously enough by making prevention integral to their business strategies? Many executives would argue that they are, after having spent more time implementing extensive corporate governance and control frameworks which are supposed to do just that. Furthermore, these frameworks are regularly reviewed by internal and external auditors, company lawyers, risk managers, compliance officers, audit committees and non-executive directors. However, in spite of tougher legislation and vociferous corporate rhetoric in recent years, not much has changed in the world of fraud and corruption. Reports of major fraud and bribery scandals are just as prevalent now as they were twenty years ago.

In support of Nigel and Samocium (2006:1), Ochonma (2015:11) maintains that control checks and measures are necessary to ensure that the value of goods and services procured is not lost through collusion between procurement officers and suppliers for the purpose of personal gain. To ensure that the capacity of procurement officers to make personal gains at the expense of the organisational gains is reduced to the barest minimum; many organisations have strengthened their ethical strategies for controlling procurement and contracting activities.

From his experience, the researcher believes that, despite massive efforts in the area of internal control, little or no progress has been made in managing procurement fraud risks. This chapter is primarily concerned with the investigation of procurement fraud. The different types of procurement fraud and how to detect, prevent and reduce procurement fraud will be discussed herein. The extent of procurement fraud and red flag indicators will also be discussed in detail in this chapter.

3.2 PROCUREMENT FRAUD DEFINED

According to Coenen (2008:86), procurement fraud is essentially the unlawful manipulation of the process of obtaining a contract for goods or services. The manipulation is aimed at gaining an advantage in the bidding or proposal process, and bad acts can range from the unfair use of insider information to the use of nefarious means to influence the process.

Coenen (2008:86) further states that procurement fraud can be broken down into three broad categories:

- Collusion between employees and vendors
  This can include kickbacks, bid rigging, gifts or other enticements.

- Vendor fraud against a company

  A vendor may commit fraud against a company by substituting goods of inferior quality, overcharging the company, or engaging in other false billing schemes.
- Collusion between multiple vendors

  Vendors may collude to artificially inflate the prices of goods and services in bids or proposals, or help one another receive certain contracts based on agreements between them.

Padgett (2015:16) defines procurement fraud as stealing items purchased, or funds intended to pay for those purchases, and covering the theft by false accounting entries. According to West (1987:23), procurement fraud can be committed by suppliers, customers or contractors in collusion with employees, through a business relationship. A typical example of procurement fraud is where a supplier submits false invoices and has an accomplice working in collusion with him to authorize the invoices for payments. Manipulation is usually confined to those documents and accounts which pass between the fraudulent company and the colluding employee as a result of their business relationship.

3.3 THE COST AND EXTENT OF PROCUREMENT FRAUD

Padgett (2015:6) emphasises that the 2011 Association of Certified Fraud Examiners' (ACFE) fraud survey indicates that governments and organisations lose an estimated five percent of their revenue due to procurement fraud each year. Procurement fraud costs businesses considerable sums of money. There is a potential global fraud loss of more than $3.5 trillion, according to the ACFE report, and the report indicates a median loss of $140,000. The average procurement fraud scheme lasted a median of 18 months before detected. According to this ACFE survey, high-risk industries are government departments and municipalities, as well as manufacturing and construction companies. This survey further indicates that the highest risk fraud activities are purchasing, supply and processing transactions. It is clear that any methodology that can be used to improve fraud risk management and reduce fraud occurrences and losses must be seriously considered.

Spollen (1997:12) suggested that the head of fraud investigation and risk management at Ernst & Young in the United Kingdom (UK) estimates worldwide fraud levels to be $10 billion per annum or $40 million per working day. Spollen (1997:11) further states that half of all procurement fraud is discovered by chance and that most fraud is committed by victim companies' own employees.

According to Corruption Watch (2013), South Africa loses about R25 billion to corruption in government procurement each year. Corruption Watch (2013) further indicate that, in 2011, Willie Hofmeyr, then head of the SIU, told Parliament that between R25 billion and R30 billion of the government's procurement budget was lost to procurement fraud and according to civil society activist Hennie van Vuuren, this is about twenty percent of the total procurement budget.

A typical example of this is South Africa's former national police commissioner, General Bheki Cele. The commissioner was suspended by President Jacob Zuma and a board of inquiry that set up to investigate him after he allegedly flouted tender processes in two lease deals for new police headquarters in Pretoria and Durban, worth R1.7bn (about £125m), by influencing the outcome of the process and ignoring the advice of procurement personnel.

According to the City of Tshwane Internal Audit Report: 2015, the CoT municipality has lost R6.2 million due to procurement fraud during 2011-2012 and 2014-2015 financial period (City of Tshwane, Forensic Investigations. Internal Audit Report (2011 to 2015), 2015:14).

3.4 TYPES OF PROCUREMENT FRAUD SCHEMES AND ITS INVESTIGATION

According to Olsen (2010:112), the most common types of procurement fraud are:

3.4.1 Kickbacks

Kickbacks are generally improper payments made to a company employee from an outside vendor. The end result is that one party gains an unfair advantage over another party through kickbacks or gifts. In these circumstances, the relationship between employees and vendors are frequently hidden.

To investigate these types of payments, expense accounts are reviewed for increased or suspicious activity, with specific attention being paid to the following types of accounts:

- Miscellaneous expense
- Commission expense
- Entertainment expense.

Padgett (2015:17) concurs with Olsen (2010:112) in stating that a ‘kickback’ is paying an employee a portion of an inflated purchase price as a reward for facilitating the deal, usually after the conclusion of the deal. Wells (2011:242) is of a similar opinion to Padgett (2015:17) and Olsen (2010:112) as he explains that kickbacks involve the submission of invoices for goods and services that are either overpriced or completely fictitious, and an employee of the company helps to make sure that a payment is made on the false invoice. For his assistance, the employee-fraudster receives some form of payment from the vendor.

3.4.2 Vendor fraud

Olsen (2010:112) confirms that vendor fraud is when fraudsters create fictitious companies and submit bills for payment to trusted suppliers who charge more than they are due. Vendors involved in fraudulent activities may even collude with employees to help them navigate through the company’s internal controls. To search and investigate this type of fraud, you could perform the following activities:

- Review vendor database for duplicate addresses
- Compare employee database to vendor database for similar addresses and names
- Identify vendor addresses that are mail drops
- Perform extensive account reconciliation
- Review journal entries
- Review invoices with missing purchase orders, duplicate or sequential invoice numbers by vendor, or duplicate date and amount
- Look for ghost/shell vendors
- Verify social security number.

Goldmann (2010:159) explains vendor fraud as when a vendor charges unusually high prices. A vendor may inflate prices for substandard goods, hoping no one in your organisation will question the discrepancies.

Albrecht, Albrecht, Albrecht and Zimbelman (2014:11) share with the views of Olsen (2010:112) and Goldmann (2010:159) by expressing that vendor fraud is perpetrated by vendors acting alone or through collusion between buyers and vendors. Vendor fraud usually results in either an overcharging for purchased goods, the shipment of inferior goods or the non-shipment of goods even though payment is made.

3.4.3 Bid rigging

According to Olsen (2010:114), bid rigging is when competitors agree in advance that one bid of many will be the winning one on a contract that a public or private entity wants to let through competitive bidding. Bid rigging generally falls into one or more of the following general categories:

- Bid suppression: agreeing to refrain from bidding
- Complementary bidding: agreeing to submit a similar but higher bid
- Bid rotation: agreeing to take turns at being bid winner
- Collusion: use of insider information to prepare and win the bid.

Since many parties can be involved in this type of fraud, it is often difficult to investigate and perform a review of a significant amount of documentation. Methods commonly used to identify bid rigging entail conducting sample reviews of bid support; performing significant analysis of variances and relationships, such as manufacturing variances; ensuring that qualified individuals review the bids; understanding how the bids are rated, reviewed, and chosen; and determining if a particular vendor(s) is consistently selected (Olsen, 2010:114).

Padgett (2015:83), who concurs with Olsen (2010:114), explains that bid rigging is any activity to suppress and eliminate competition on contracts. Bid rigging is an agreement where, in response to a call or request for bids or tender, one or more bidders agree not to submit a bid, or two or more bidders agree to submit bids that have been prearranged amongst themselves. Profits will be shared.

Bid rigging includes agreement to restrain competition in making bids and agreement to refrain from bidding, agreements to fix prices, to submit identical prices, to rotate winning bidders and/or to share profits (American Bar Association, 2008:114).

3.4.4 Defective pricing and price fixing

According to Olsen (2010:114), defective pricing occurs when a contractor does not submit or disclose cost or pricing data that is accurate, complete, and current prior to reaching a price agreement. Olsen (2010:115) defines price fixing as an agreement amongst competitors to raise, fix, or otherwise maintain the price at which their products or services are sold.

To detect and prevent these types of schemes, one could take the following actions:

- Test transactions for circumvention of controls or safeguards by activities such as manual overrides
- Ensure separation of power in the approval and payments processing of invoices
- Perform market research to compare prices with industry standards
- Perform selected background checks to identify personal relationships between employees negotiating contracts and vendors.

Cascarino (2013:17) and Olsen (2010:115) are of the opinion that price fixing is an anti-competitive activity involving an agreement amongst competitors to fix prices, thus colluding to inflate prices and cheat customers. Typically, price fixing is an agreement amongst competitors to fix, raise, or simply maintain a price at which the goods and services are sold. Cascarino (2013:20) further maintains that defective pricing involves contractors inflating their costs in order to increase profits or limit their losses.

3.4.5 Conflict of interest

Padgett (2015:23) confirms that conflict of interest is a situation that has the potential to undermine the impartiality of an individual because of the possibility of a clash between the individual’s self-interest and professional or public interest. This confirms the view of Vanasco (1997:117) who explains that conflict of interest arises when employees are both self-employed and work, at the same time, with organisations. They frequently tend to sell their personal products to the organisations for which they work. Wells

(2011:255), who is in agreement with Padgett (2015:23) and Vanasco (1997:117), suggests that conflict of interest occurs when an employee, manager, or executive has an undisclosed economic or personal interest in a transaction that adversely affects the company. The researcher has previous experience in the investigation of matters related to procurement fraud and contends that, apart from the above five mentioned types of procurement fraud schemes, there are many other schemes such as split purchases, duplicate payments, product substitution and fictitious transactions that investigators must be aware of.

3.5 DETECTION AND PREVENTION OF PROCUREMENT FRAUD

Olsen (2010:119) suggests that a more cost-effective approach to addressing procurement fraud is to take proactive steps. Preventative action can include steps similar to those one would take to establish or enhance internal controls and corporate compliance guidelines. According to Olsen (2010:119), the following are some specific steps that can be implemented to assist in the detection and prevention of future occurrences of procurement and related fraud:

- ***Segregation of duties***: more than one person creating orders, receiving invoices, making payments
- ***Supervisory controls***: someone is watching
- ***Receiving controls***: who is receiving the invoices, and who is receiving the goods?
- ***Authorisation controls***: how many people sign the checks?
- ***Reconciliation controls***: how frequently are bank statements reconciled to books and records, and by whom? Are they independent of other payable functions?
- ***Recording controls***: does a well-defined and logistical documentation process exit?
- ***Communication and training of employees***: Does everyone know what they should be doing?

- ***Defined reporting lines and investigative measures***: do employees know the consequences of their actions and to whom they answer?
- ***Consistent policies***: prevention can be aided through consistent policies and procedures across an organisation, especially if the organisation procures goods from many suppliers in different industries and countries.
- ***"Don't hide behind it!":*** prosecute employees for fraud. Most companies are too embarrassed to take action for fear of bad publicity or damage to the company's image. However, procurement fraud is probably the least visible to detect and most costly for the organisation or company.

West (1987:111) points out that reduction, prevention, detection and recovery measures can be implemented through the installation of protection equipment and software. They can also be implemented by the appointment of control and security personnel, by setting up control and reporting procedures, or by providing security training to improve general awareness of risks, and taking effective action to minimize losses. West (1987:112) further mentions that computer models to detect procurement fraud can be designed by the computer auditor so as to facilitate the policing of an organisation's business activities. These would help to spot abnormal activities more quickly and enable action to be taken in order to curtail further damage to the organisation. In support of Olsen (2010:119), West (1987:111) explains that failure to appreciate the need for proper segregation of duties in key functions has resulted in many procurement frauds being successful.

In his study, Vanasco (1997:118) shares a similar opinion as Olsen (2010:119) and West (1987:111) by claiming that, in order for investigators to detect potential procurement fraud, auditors use Computer Assisted Auditing Techniques (CATTs) which allow the auditors to compare:

- Vendor addresses to employee address
- Vendor address to employees' outside business addresses; and
- Vendor telephone numbers to employees' home telephone numbers or outside business numbers.

Coenen (2008:123) concurs with Vanasco (1997:118), Olsen (2010:119) and West (1987:111) by explaining that twenty five percent of all procurement fraud is detected by accident. One logical way to actively look for procurement fraud within a company is through its computer systems. Sophisticated software can track and log computer activities, and companies would be wise to track computer login attempts, password attempts, and data access attempts. Unusual activity in any of these areas can signal a procurement fraud risk, and tracking these things is simple once that software is in place.

3.6 PROCUREMENT FRAUD RED FLAGS

Red flags are sets of circumstances that are unusual in nature and vary from normal activities. They represent a signal that something is out of the ordinary and may need to be investigated. Red flags do not indicate guilt or innocence but merely provide possible warning signs of procurement fraud (Padgett, 2015:73).

Padgett (2015:77) lists the following red flags of procurement fraud:

- Increasing number of complaints about products or services
- Increase in inventory purchased but no increase in sale
- Charges without shipping documents
- Payments to vendors who are not on an approved vendor list
- High volume of goods purchased from new vendors
- Purchases that bypass the normal procedures
- Vendors without physical address
- Vendor address matching employee address
- Purchasing agents who pick up vendor payment rather than having them mailed.

Coenen (2008:58) mentions that a company's poor record keeping encourages procurement fraud because employees know that information is not being properly recorded and evidence of fraud may be easy to conceal. Coenen (2008:58) further lists the following documentation red flags that might be useful to investigators:

- Missing or altered documents
- Evidence of backdated documents
- No original documents available
- Questionable signatures on documents.

According to the SIU Training Manual (2010:149-150), the procurement fraud investigator might find it useful to look out for the following “red flag” payments during his/her investigation:

- Suppliers who submit more than one invoice on the same day
- Invoices which are in sequence and received from the same supplier
- Duplicate payments
- On the same dates, the same amounts with the same invoice numbers are paid to different suppliers
- Invoices dated on weekends or public holidays
- Invoice amounts which are higher or lower than the payment amount
- Invoices with no payments
- Payments with no invoices
- Suppliers using the same invoice number
- Order numbers which are in sequence
- Orders which are in sequence on the same day
- Suppliers who use more than one account number
- Bank account details which constantly change
- Round amount payments
- Payment amounts from R29 000,00 to R29 999,00 (these amounts are just below the delegation and can indicate possible splitting of transactions)
- Invoices which are repeated and paid twice.

It is worth noting that employees living beyond their means exhibit key red flags. Lifestyle audits must be conducted on employees who openly live beyond their means.

Sudden behavioral changes are examples of red flags for fraud. An employee who boasts about significant new purchases and carrying unusually large sums of money is indicating the red flag for fraud.

3.7 INVESTIGATION OF PROCUREMENT FRAUD

According to Wells (2011:365), after procurement fraud has been detected, a thorough investigation is required as it can help a company or organisation to reduce its losses, identify the fraudster, and recapture some of or the entire amount stolen. It also sheds light on weaknesses in the company's control structure, thereby helping to shore up the company's internal defenses against future procurement fraud. Golden, Skalak and Clayton (2011:433) confirm that procurement fraud investigation will begin with the investigation of vendors, which should focus on where the money went and for what purpose. All relevant disbursement information should be collected.

Wells (2011:366) further emphasises the following primary requirements of procurement fraud investigation:

3.7.1 Planning the investigation

Planning will start with the selection of an investigation team and outlining their responsibilities. When choosing an investigation team, it is critical to identify those who can legitimately assist in the investigation and those who have a genuine interest in the outcome of the investigation. Wells (2011:367) further mentions that a procurement fraud investigation team must include the following types of professionals:

- **Certified fraud examiners (CFE):** A CFE is trained to conduct a complex fraud examination. Procurement frauds frequently present special problems because they require an understanding of complex financial transactions as well as traditional investigative techniques. A CFE has training in all aspects of a fraud examination and can therefore serve as a valuable "hinge" to the investigation team.

- **Legal Counsel:** It is crucial to have a counsel involved in the procurement fraud investigation as this type of investigation can be a veritable hornet's nest of legal questions. In addition, by having a counsel directly involved in the investigation, the company may be able to protect the confidentiality of its investigation under attorney-client privilege and the work-product doctrine.

- **Internal Auditors:** Auditors are frequently the people who detect financial anomalies that lead to procurement fraud investigations. They are liable to identify fraud indicators and to help with designing procedural methods to identify the perpetrators as well as the extent of fraud.

- **IT and computer forensics experts**: In almost every procurement fraud case, a computer was involved. A computer may have been used to alter legitimate documents or to send or receive e-mail. IT personnel can help identify what data is available for investigation and where it is located. IT should form part of the team in order to safeguard data until it can be analysed. Computer forensics experts should be used to capture and analyze digital data. Because electronic data can be easily altered, only trained professionals should be used to secure data so that it can be analyzed more thoroughly without disturbing the original files.

- **Human resource personnel**: The human resource department should be consulted to ensure that laws and policies governing the rights of employees in the workplace are not violated. Such involvement will minimise the possibility of a wrongful discharge suit or other civil action by an employee.

- **Management representative**: A representative of management should be kept informed of the progress of the investigation and should be available to lend necessary assistance. A sensitive procurement fraud investigation has virtually no hope of success without strong management support.

- **Outside (independent) consultant**: In a case wherein a suspect is an employee who is powerful or popular, it might be useful to employ outside specialists who are relatively immune from company politics or threat of reprisal. In addition, some investigatory procedures, such as forensic documents analysis, require a high level of proficiency and expertise and should therefore only be undertaken by professionals who are specifically trained in that field.

McMillan (2006:109) puts forwards that once the investigation team has been assembled, they work out the details of the investigation plan based on what is known about the incident at the time. Details, of course, may change once field work has commenced and more information becomes available.

Coenen (2008:130) indicates that the first step in a full-blown procurement fraud investigation is creating a team of qualified professionals. Some team members may be employees of the company, while others might more appropriately be outside consultants.

3.7.2 Developing evidence

According to Wells (2011:369), once it has been determined that an investigation is warranted, the investigation team will design procedures to collect and develop evidence. Evidence is anything perceivable by the five senses, including any proof, such as testimony of witnesses, records, documents, facts, data, or tangible objects that are legally presented at trial to prove a contention and to induce a belief in the mind of a judge. The evidence can be gathered in one or more of the following ways:

- **Subpoenas:** Is an order from court issued to a suspected employee or vendor to produce documents and records (including electronic records). It can also be used to obtain witness evidence and statements.
- **Search warrants:** If there is probable cause to believe that certain documents and records have been used in the commission of procurement fraud,

investigators will apply for a search warrant to search and collect the required documents, and the computer used by the suspected employee.

- **Voluntary consent:** Documents can be obtained by voluntary consent. This is often the simplest means to obtain documentation and it is therefore the preferred method in many investigations. While consent can generally be either oral or written, it is recommended that the consent be acknowledged in writing.

- **Interviewing witnesses and employees:** In the procurement fraud investigation, there is nothing more important to the successful resolution of the case than the ability to conduct a thorough interview of witnesses. In light of the above, and as indicated by Schwartz (2010:2), interviewing employees can be useful in discovering potential procurement fraud. Interviewers sometimes find that employees have information about potential inappropriate relationships between employees and vendors or are suspicious about certain transactions. Interviews at all levels within the company can give insight into the daily operations of the company and can reveal fraud risks which may be otherwise unknown to the organisation.

- **Background checks:** According to Schwartz (2010:2), background checks can provide information on the background, integrity, and reputation of selected individuals and entities. A small amount of time spent performing a background investigation might reveal connections between employees and vendors. In addition, it can provide a history on vendors’ performance, legal proceedings, and other relevant information.

- **Electronic discovery:** Electronic discovery, such as extracting and analysing email files, can identify any questionable correspondence between vendors and employees using an organisation’s computers (Schwartz, 2010:2).

Golden et al. (2011:434) state that the following critical information must be collected:

- Vendor information setup in the company's master file data for the accounts payable system
- Contracts, purchase orders, invoices, and documents used to accumulate payment approvals, receiving documents, correspondence concerning credits, billing errors, or other matters
- Internal reviews of vendor quality and the results of public record searches performed to qualify the vendor.

In addition, Golden et al. (2011:434) indicate that the collection of the above mentioned items is likely to be facilitated by computer forensics techniques such as data mining for duplicate addresses, similar names, or duplicate payments, invoices, or purchase orders, among other queries.

3.7.3 Preserving evidence

Wells (2011:371) indicates that even if the investigator is careful to obtain the evidence legally, the case can be lost if the investigation team fails to preserve the evidence so that it is accepted by the court. For evidence to be admissible, basic procedures in its handling must be followed. The evidence submitted must be properly identified, and it must be established that the proper chain of evidence was maintained. In addition, proof must be provided that the evidence is relevant and material to the case. The following general rules should be observed with regard to the collection and handling of documents:

- Obtain original documents when feasible. Make working copies for review; keep the original segregated.
- Do not touch originals any more than necessary; they might later have to undergo forensic analysis.
- Maintain a good filing system for the documents. This is critical, especially when large numbers of documents are obtained. Documents can be stamped sequentially for easy reference.

In support of this, Golden et al. (2011:435) suggests that original documents should be marked as evidence and filed separately. Investigators must obtain permission to remove the original documents from the site.

3.7.4 Organisation and analysis of evidence

Wells (2011:373) posits that it is essential that any documents obtained be properly organized early in an investigation, and that they be continuously reorganized as the case progresses. McMillan (2006:116) agrees with Wells (2011:373) by emphasizing that it is very important to document and safeguard the originals by placing them in a secure safe and to only work on copies. Safeguarding the evidence also prevents tampering with originals before actual analysis.

Wells (2011:373) further maintains that good organisation in complex fraud cases includes the following:

- **Segregation:** segregating documents by either witness or transaction.
- **Chronologies:** a chronology of events should be commenced early in the case in order to establish the chain of events leading to the proof. Keep the chronology brief and include only information necessary to prove the case.
- **To-Do lists:** the list which must be updated frequently should be kept in a manner that allows it to be easily modified and used as a cumulative record of investigation tasks.
- **Using computer software to organize documents and other data:** computers are one of the most valuable tools for fraud investigation. Use of a computer database enables investigators to easily store and access pertinent information about the case and the documents that have been assembled. Special software can be used to sort, chart, and graph the information in the database, making it easier to analyze relationships and identify anomalies. The following are a few of the software programs commonly used for case management and reporting:

    - I2 Analyst’s Notebook
    - CaseMap by CaseSoft
    - NetMap by Alta Analytics
    - MAGNUM Case Management Software
    - Watson and PowerCase from XANALYS.

Coenen (2008:134), who shares with the view of Wells (2011:373), explains that good document management procedures are critical, especially in an investigation that is document intensive. Coenen (2008:134) recommends that organizing documents chronologically, and possibly also separating them by witness or transaction, together with maintaining a computer database or spreadsheet for tracking documents, is also helpful.

3.7.5 Report writing

Wells (2011:374) confirms that the investigation will conclude with reporting the investigation findings and results, for which a formal written report will be drafted and submitted to the management. Such a report is normally used for internal disciplinary hearings to be instituted but may also be used for complaints to the SAPS Commercial branch or SIU, or claims to insurance companies.

Furthermore, Wells (2011:374) mentioned the purpose of the investigation report as to:

- **Convey evidence**: the written report communicates all evidence necessary for thorough and proper evaluation of the case.
- **Add credibility**: because the written report is completed in a timely manner, it adds credibility to the investigation and can be used to corroborate earlier facts.
- **Accomplish objectives of case**: knowing that a written report must be issued after the investigation is completed, the report forces the investigator to consider his actions beforehand.

In this respect, McMillan (2006:110) explains that after completion of the investigation, a written report must be prepared, summarising the incident, and supported by details gathered during field work. Coenen (2008:139) agrees with McMillan (2006:110) and Wells (2011:374) by pointing out that a procurement fraud investigation is most often concluded with a written report that details the findings of the investigation.

3.8 SUMMARY

This chapter established that procurement fraud is rife across the globe, resulting in a loss of billions of dollars annually. However, with proper internal control and investigation, the reality of reducing the risk of procurement fraud is achievable in an organisation. Any organisations that believe they can operate and grow without good internal controls and without an effective internal audit are making a serious mistake. Such organisations are at an increased risk of procurement fraud. Effective controls, which can save the company a fortune, can be established relatively quickly and at a reasonable cost. An affective internal audit is the only way to tackle the risk of procurement fraud.

To ensure that an internal audit is effective, management should clearly set out the policies and procedures by which the business of the company is to be conducted and they should give the internal auditor the authority and scope to do its job and reflect this in its reporting lines. Internal auditors must have a deep understanding of procurement fraud, focus on the risks thereof, work closely with external auditors and regulators in creating a control-conscious environment. Every organisation should have properly documented policies and procedures. Without clearly and constantly updated policies and procedures, which cover all facets of the business, companies leave themselves open to the risk of procurement fraud.

When setting up a team, the investigation team should be limited to only those persons who are vital to the investigation process. The purpose of an investigation is to gather evidence to prove or disprove the allegations of fraud. Once evidence has been gathered, the investigator must take care to properly preserve the evidence so as to ensure its admissibility in a court of law. The organisation of evidence is also crucial. Several computer software programs are available to aid investigators with case management and reporting. Procurement fraud investigation will generally conclude with a formal written report of the findings of the investigation.

Chapter Four, provides a presentation and discussion of the research findings of this study.

CHAPTER FOUR
PRESENTATION AND DISCUSSION OF THE RESEARCH FINDINGS

4.1 INTRODUCTION

In this chapter, the interpretation of the qualitative data (from semi-structured individual interviews, as discussed in section 1.10 of Chapter One) is presented and discussed by means of themes, to indicate the achievement of the aim, purpose and research questions of this study, as indicated in sections 1.5, 1.6 and 1.7 of Chapter One. In order to realise these goals, fifteen semi-structured individual interviews were conducted with CoT forensic investigators involved in the investigation of fraud within the CoT municipality. In order to promote the trustworthiness of the study, the research methodology (as discussed in section 1.14 of Chapter One) was implemented and adhered to in the collection and analysis of the data.

During the process of data collection, that is, the semi-structured interviews, the interview questions, reflected in Annexure A, were used to structure and guide the discussion. The respondents' feedback to these questions was subjected to data analysis by the researcher and the main themes, as discussed below, emerged.

The outcomes of the individual interviews are presented below.

4.2 THE OUTCOMES OF THE INDIVIDUAL INTERVIEWS

This segment of the dissertation provides a detailed explication of the main themes that emerged from the collected data. Each theme is discussed as a separate item, with each discussion substantiated by the use of verbatim quotes from the transcribed interviews. For each section, the thematic analysis begins with a depiction of the theme, which is elaborated upon and supplemented by the interviewees' responses to the questions. Finally, subsequent to the presentation of each theme, an appraisal is presented, which concludes the discussion of each theme. The questions posed to the respondents are provided, followed by the interpretation of the responses to the questions, which will be enriched by direct verbatim reflections of the responses.

4.2.1 Gender of respondents

From a total of 15 respondents, 8 (55%) were male, while 7 (45%) were female.

Table 4.1: Gender of participants

Total number of respondents: 15		
Gender	**Number**	**Percentage (%)**
Male	8	55
Female	7	45

4.2.2 Respondents' period of employment in the CoT Forensic Services

The table below presents the period of employment of the respondents.

Table 4.2: Respondents' period of employment in the CoT Forensic Services

Total number of respondents: 15			
Key	**Number of years' experience**	**Respondents**	**Percentage (%)**
0–5	Between 0 and 5	10	66,6
6–10	Between 6 and 10	3	20
11–15	Between 11 and 15	1	6,7
16–20	Between 16 and 20	1	6,7
>20	More than 20	0	0

4.2.3 Divisions/units to which respondents are designated

The table below presents the divisions/units to which the respondents are attached.

Table 4.3: Divisions/units to which respondents are designated

Total number of respondents: 15		
CoT divisions/units	**Respondents**	**Percentage (%)**
Forensic Services	15	100

4.2.4 Formal training attended by respondents

The table below presents the formal training attended by the respondents.

Table 4.4: Formal training attended by respondents

Total number of respondents: 15		
Training/course	**Yes**	**No**
Computer forensics	04	11
Cyber forensics	03	12
Digital forensics	02	13
Procurement fraud investigations	09	06

The first theme to be discussed is the application of computer forensics in forensic investigation.

4.3 THE APPLICATION OF COMPUTER FORENSICS IN FORENSIC INVESTIGATION

Computer forensics is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is acceptable in a legal proceeding. The computer forensics process requires a vast knowledge of computer hardware and software in order to avoid the accidental invalidation or destruction of evidence and to preserve the evidence for later analysis. A computer forensics review involves the application of investigative and analytical techniques to acquire and protect potential legal evidence. Therefore, a professional within this field needs to have a detailed understanding of the local, national and international laws affecting the process of collection and retention of computer evidence. This theme provides an understanding of the respondents' knowledge and views on the application of computer forensics in forensic investigation.

4.3.1 Understanding of the term ‘computer forensics’

Computer forensics is a very complex enterprise which requires a vast amount of computer knowledge and expertise. As the world of computers evolves and the challenges related to cybercrimes are on the rise, law enforcement agencies must also accelerate their cyber techniques to catch up and counter attack this global dilemma. Computer forensics involves the use of sophisticated technology tools and procedures that must be adopted and applied at all times to guarantee the precision of the collection and preservation of evidence and the accuracy of results concerning computer evidence processing and analysis.

In this regard, the respondents were asked to respond to the following question: *What is your understanding of the term ‘computer forensics’?*

The objective of this question was to establish the extent of the respondents' understanding of the term ‘computer forensics’. Respondents were probed as to whether they fully understand the term ‘computer forensics’. The majority, thirteen respondents, said that computer forensics is the collection, extraction, analysis and reporting of digital data. One respondent indicated: *My understanding is the ability to extract, [INDISTINCT]… source, analyse information related to an investigation of evidence from a computer system.*

Another respondent expressed that computer forensics deals with an investigation concerning computers and anything embedded on them: *For me, computer forensics is when you deal with investigations concerning anything that is embedded on a computer, anything which is automated, anything which runs on a computer. Then you have to interrogate how the system works, how the system was designed, and how the system can be manipulated to carry out fraud which is basically on the computer. That, to me, is computer forensics and also the same thing as cyber because cyber is things that happen on the computer and they happening behind the computer if [INDISTINCT] you have the [INDISTINCT] in the clouds you don't even know what's happening.*

It is clear from the participants' responses that the majority of them understood the term computer forensics as the collection, preservation and analysis of digital evidence. The researcher shared the same sentiments as the participants in terms of the definition of computer forensics, as indicated above.

4.3.2 Objectives of computer forensics

For investigators to achieve what they intend to achieve, when they apply computer forensics, they first need to understand the objectives of computer forensics. These objectives are to recover, analyse, and preserve the computers, digital evidence and any other related digital materials in a manner that can be presented as evidence in a court of law.

The respondents were asked to respond to the following question: *What are the objectives of computer forensics?*

Six participants were of the view that the objectives of computer forensics are to identify, extract and recover, collect, analyse and preserve digital evidence for court purposes. One participant expressed that *the objective of a computer forensics would be to extract information that can be used as evidence that is admissible and that you can testify to the authentication of that information that you extracted from the computer and that no changes were done during the course of the analysing and extraction of the information.*

Similarly, another respondent stressed that the objectives of computer forensics are to identify data, retrieve it using computer software, as well as to collect, evaluate and preserve the data for court purposes: *the objectives - identifying data that is collected electronically by retrieving it from a computer using computer softwares [sic] and evaluating information or data that was recovered and also preserving those image [sic] for court purpose.* Eight respondents stated that they do not know the objectives of computer forensics.

It is of paramount importance that the forensic investigator knows and understands the objectives of computer forensics before beginning with the investigation, as it will give them a sense of what they are going to do. During the interviews, it became apparent that there is a lack of comprehensive understanding of the objectives of computer forensics amongst the majority of the participants. This illustrates that the CoT investigators do not know exactly what to do when investigating computer-related crimes.

4.3.3 Four-step process of computer forensics investigation

For every computer forensic investigation, investigators are required to properly and legally identify, preserve, collect, evaluate or analyse, document and present all the data. Otherwise, it will be fruitless at the end of the day as the validity and reliability of that data will virtually be tested or disputed in a court of law.

The study respondents were asked to respond to the following question: *Are you familiar with the four-step process of computer forensic investigation? If affirmative, briefly name these steps. If not, motivate why not?*

There was consensus amongst eleven of the respondents, who indicated that the four-step process of computer forensic investigation incudes: acquisition, examination, analysis and reporting. One respondent answered: *I would say yes. It will be collecting the device that you going to collect information from. It will be using a specific tool to extract data information on that. And it will be the manner in which you will be imaging that computer and preserving it for future usage in court.*

Furthermore, two of the respondents expressed that the four-step process entails collection, which involves extraction, recovery, examination, analysis and then compiling of a report. One respondent was of the following opinion: *Ja. The four-step will be…it's the normal steps because it will be mostly the collection which involve extraction and also recovery, there's examination of the data, there's also analysis after examination, and then compiling a report.*

The four-step process of computer forensics is arguably the most important and cannot be overlooked. If it cannot be done properly and legally the validity and reliability of the data will be questionable. In addition, the majority of the respondents showed an understanding of the four-step process of computer forensics.

4.3.4 Application of computer forensics in procurement fraud investigations

Most, if not all, procurement fraud investigations involve computer systems. This implies that computer forensics should be applied for each and every procurement fraud investigation.

The respondents were asked to respond to the following question: *Have you previously applied computer forensics in procurement fraud investigations? If affirmative, did it add value to the investigation? How? If not, why not?*

Interestingly, ten respondents confirmed that they had previously applied computer forensics in procurement fraud investigations. One respondent submitted this response: *yes, I have used computer forensic in some cases. We were required to go through some transaction [sic] for some fraudulent activities. Also I was helping in the [INDISTINCT] if I may say and, yes, it did add value because we managed to identify a quite number of transactions that were not done according to the processes that are in place. We also managed to identify the people who were busy manipulating those transactions [sic] and it was easy to detect and to identify those individuals. We also collected evidence using computer forensics that directly point to the suspected individual [sic] that were alleged to be conducting those transactions. So, in full, yes, it did add value.*

Similarly, another respondent highlighted that she had previously applied computer forensics to link the buyers to the service provider: *yes, I did. It did add value in a way that we were able to link buyers to the service provider and proving that fraud was committed.*

In contrast, five respondents emphasised that they have not previously applied computer forensics in a procurement fraud investigation. One respondent in particular expressed that *personally no. I've never…like I've said, and I'll say it again, I've never* *really worked on a case that requires forensic fraud because I don't have the training and the expertise in that. I only assisted in some cases.*

It is worth noting that one needs to be involved to learn and gain experience. The researcher shared the same sentiments with those who urged that computer forensics add value to the procurement fraud investigations that they had previously investigated.

CoT investigators who are not well trained or have not applied computer forensics during procurement fraud investigation spend more time than required, that is, three months, to investigate and finalise a case. This results in them losing those cases.

4.3.5 Steps that a computer forensics investigator should follow to preserve digital data for future computer forensics examination

Computer forensics data must be properly collected and preserved to be used in court. If the data is not properly preserved, it may be inadmissible. The computer forensics process is built around the fact that computer evidence was not altered, tampered with, or destroyed. Computer forensics data that was not appropriately handled will attract significant rebuttal in court. Computer data is evidence that does not die and, if properly collected and preserved, it guarantees a conviction.

The respondents were asked to respond to the following question: *Are you conversant with the steps that a computer forensics investigator should follow to preserve digital data for future computer forensics examination? If affirmative, briefly list these steps. If not, motivate why not?*

Nine respondents indicated that they are familiar with the steps that a computer forensics investigator should follow to preserve digital data for future computer forensics examination. These nine respondents expressed the view that forensic investigators must make a copy of the evidence and avoid tampering with evidence, and that they should not allow anyone to have access to it. One respondent submitted the following: *I* *can try to explain what I know. You need to seize the computer. Then you need to extract the information from the original hard drive of the computer to a secondary hard drive which you will use to analyse the information and do analytical reviews to extract the information and to go through the information and…without tampering the original hard drive. And then this can be used…the secondary hard drive can be used to analyse and to present and to extract the information.*

Five respondents indicated that they are not familiar with the steps that a computer forensics investigator should follow to preserve digital data for future computer forensic examination. One respondent stated: *I have only yet been offered with the training and I assume that that is not something I can do on my own without the relevant knowledge.*

It is pointless to collect digital data and fail to properly preserve it as it will be inadmissible in court. It is important to guard against anyone who can alter, tamper with or destroy the computer forensic evidence. The CoT investigators who are not familiar with the steps that need to be followed to preserve digital data tend to tamper with and destroy digital evidence, which leads to disputes being raised during criminal trials or disciplinary proceedings and casts doubt on the credibility of the evidence presented.

4.3.6 Chain of custody of evidence seized during computer forensics investigation

Chain of custody is a record of all the individuals who came into contact with computer forensics evidence. Chain of custody establishes proof that the data that was collected at the crime scene is the same data that is being presented in a court of law.

The respondents were asked to respond to the following question: *Are you familiar with how to maintain the chain of custody of evidence seized during a computer forensics investigation? If affirmative, briefly indicate how you maintain chain of custody? If not, motivate why not?*

From the responses to this question, seven respondents highlighted that evidence must be sealed in a bag, photos must be taken, the bag must be numbered and/or tagged, whoever accesses the evidence must have the proper authorization, he/she must sign with the date, time and place where the evidence is being accessed, and provide a reason why he/she is accessing the evidence. Furthermore, five respondents expressed that there must be a proper register and record-keeping of the evidence indicating the time, date and person who takes possession of the evidence: *I believe that it will not be any different from any other evidence. So those steps will be that when you confiscate or take possession of any evidence there must be a proper register for that. When that evidence is being given to any other person or any other third party, it must also go through a proper record-keeping system by indicating the time, the date, the person who signed for it, and the reasons for that purpose of containing that evidence.*

It also came to light, from three respondents, that whoever is handling the evidence must sign for it and he/she must mention the dates, time, place, name of the person who is signing for it, and obtain their signature: *Yes. When seizing evidence from computer, or whatever device, you must make sure that there's witnesses. You must make sure that you hand…the handing and delivering part of it you sign for that and it must mention the dates, it must mention the time, the place, who is signing for that, and signature as well. And you must make sure that you package it in a manner that it will not contaminate the evidence and seal and if there's some…if your sealing method has some numbering or names you must make sure that you also put that on your log-sheet and whoever that you going to hand it over to they must also sign and it must be stored in a safe place 'til the time when it's needed to be used. If it's papers you must make sure that you don't punch holes, you don't staple them, and…that is [CROSSTALK]. You must retain them as original as possible.*

Computer evidence will change hands or locations before it gets presented in court. It is collected, logged in at the lab, stored, checked out for analysis and checked back in for storage. Each of these steps must be documented and accounted for; without this detailed account, the evidence will be deemed untrustworthy and inadmissible.

4.3.7 Basic qualities of a computer forensics investigator

A computer forensics investigator is someone who has a vast amount of investigative experience and knowledge to conduct computer-related investigations. This is someone who is qualified to conduct investigations involving computers and software, and any other technological matter.

The study respondents were asked to respond to the following question: *According to you, what are the basic qualities that a computer forensics investigator should have?*

The respondents unanimously agreed that the basic qualities of a computer forensics investigator are: problem solving skills, analytic skills, familiarity with computers, investigative skills, passion for IT, knowledge of law of evidence and being a constant learner. One respondent was of the view that a computer forensics investigator needs to have a good understanding of how a computer or a computer system works: *They need to know…they need to have a good understanding how a computer or a computer system works. They need to know…they need to stay updated with the changing environment. They need to know…and know how to work the basic software that goes with it. You need investigation skills when collecting information or even collecting the hard drive or the computer itself. And then you need analytical skills and also reporting skills. And when you testify in a court of law or a disciplinary action you need to know what you are supposed to testify about and what not.*

Moreover, the respondents highlighted that a computer forensics investigator must have a passion for IT and be very analytical: *You must have a passion for IT. You must have a passion for [INDISTINCT – bursting?] crime. You must be very analytical. You must understand what it is that you are going through to work with. And you must be a person who is a constant learner. Why I'm [sic] saying that because the IT environment is constantly evolving so you must be a constant learner. You cannot afford to say I learnt two years ago. You'll become ineffective. So, for me, you've got to be a constant learner. Those are the basic qualities that I would look for. And someone who understands forensics completely. For me, someone also who understands the financial* *background of how things happen. That is very important because most fraud is about financial benefit in [INDISTINCT].*

In respect of this, the researcher concurs with the respondents when stating that a computer forensics investigator should have a very good memory for facts, names, places and dates, and should be innately curious and a constant learner.

4.3.8 Computer forensics investigation training

Training and skills development in any organisation should be a continuous process. The training and skills provided to the CoT forensic investigators should prepare and educate them to efficiently deal with computer forensics investigations.

The respondents were asked to respond to the following question: *In your opinion, have you received sufficient training to confidently conduct effective computer forensics investigations? If not, how could your efficiency as a computer forensics investigator be improved?*

All, except one, respondents indicated that they did not receive sufficient training to confidently conduct effective computer forensics investigations. Fourteen respondents shared the sentiment that, for their efficiency to be improved, they need training in computer forensic investigations. One respondent stressed that he needs the right training in order to improve his efficiency in dealing with computer forensic investigations: *Training and the right training because unfortunately forensic investigations it's not just a methodology. There is a lot of technical skills.* Another respondent also expressed that she needs computer courses and training*: Through courses, computer forensic courses, and trainings.*

In contrast, one respondent indicated that he has received sufficient training to effectively conduct a computer forensic investigation. He indicated that *sufficient training. I would say so. I'll say –…to computer forensics I'll say I have.*

It was confirmed by the majority of the participants, during the interviews, that training opportunities and a learning environment must be created by the CoT municipality, so that their efficiency and success in dealing with computer forensics investigations are improved.

Lack of sufficient training is one of the major contributing factors to the CoT forensic investigators not being able to efficiently and successfully deal with computer forensic investigations.

4.4 AN OVERVIEW OF THE INVESTIGATION OF PROCUREMENT FRAUD

Procurement fraud is arguably one of the greatest unmanaged commercial risks of all time. Highest-risk industries are government departments and municipalities, as well as manufacturing and construction companies. The most frequent targets for procurement fraud activities are purchasing, supply and processing of transactions.

Procurement fraud can be committed by suppliers, customers or contractors in collusion with employees through a business relationship.

4.4.1 Understanding of the term ‘procurement fraud’

To successfully deal with procurement fraud, forensic investigators should have a clear understanding of the term ‘procurement fraud’, which is the manipulation of the procurement process in order to gain an advantage over other bidders or suppliers.

The respondents were asked to respond to the following question: *What is your understanding of the term ‘procurement fraud’?*

The resounding response to this question, from all the participants, was that procurement fraud is the unlawful manipulation of procurement processes. One respondent indicated that procurement fraud is the manipulation of the process of procurement: *Procurement fraud. I will say it's when people are manipulating the process of procurement mostly by overriding or just ignoring controls are in places to safeguard or to ensure that all procurement processes are adhered to.*

Another respondent also emphasised that procurement fraud is the unlawful manipulation of a process to acquire goods or services: *It's unlawful and manipulation of process to acquire goods or services to obtain an unfair advantage.*

4.4.2 Types of procurement fraud

For the effective investigation of procurement fraud, it is important that the CoT forensic investigators are familiar with different types of procurement fraud. It is, however, the responsibility of the CoT to empower its forensic investigators with the required knowledge to familiarise themselves with different types of procurement fraud.

The respondents were asked to respond to the following question: *Are you familiar with the different types of procurement fraud? Briefly list these types of procurement fraud?*

It was made clear by fourteen respondents that the following are different types of procurement fraud: splitting of quotations, collusion between employees and suppliers, conflict of interest, kickbacks, fictitious transactions, price fixing and no rotation of suppliers. One respondent listed bid rigging as the most popular type of procurement fraud: *The most popular one now is [INDISTINCT] tendering which is bid rigging. The other one will be collusion between procurement staff and service providers. You'll have improper selection of suppliers which will be no rotation of suppliers, favouring other suppliers over others. Another one, procurement will be just simply ignoring that…those controls that are there to stop this kind of dealings in the procurement sector. Another one would be [INDISTINCT] where a person actually give [sic] information to service providers to give them an edge when they are tendering or maybe in the competitions bidding. That's about it.*

It was further expressed, by another respondent, that another type of procurement fraud is the inflation of prices to accommodate kickbacks: *One type of procurement fraud is…let's say, for example, tenders are advertised so that people apply and whoever gets appointed…so there is rigging in that process. So people who are not supposed or don't qualify or came late but are entered into the process and are eligible and [INDISTINCT]. So that there's the rigging part of it. And then, secondly, there's a type of fraud where there's inflation of prices to accommodate kickbacks and so forth. So if a [INDISTINCT] person responded to a tender, applied on time, it's allocated nicely, but they inflate the prices. Businessman does not necessary want to pay a bribe.*

The researcher agreed with the respondents when they indicated that there are many other types of procurement fraud, such as split purchases, duplicate payments and product substitution, that the CoT forensic investigators must be aware of.

4.4.3 Processes of procurement fraud investigation

For any investigation, it is important for the forensic investigators to follow certain processes in order to achieve the aim and scope of the investigation. The same applies to procurement fraud investigation.

Respondents were asked to respond to the following question: *According to you, what are the processes of procurement fraud investigation? Briefly name these requirements?*

Ten respondents were of the view that the processes of procurement fraud investigations are planning, gathering evidence, conducting interviews, evidence analysis and drafting the report. One respondent suggested that, after the planning phase, fieldwork needs to be conducted in order to gather evidence to support the allegations. Further, the respondent indicated that interviews should be conducted, and analyses of the evidence, then a report should be submitted on the findings:

First one will be understanding of the procurement processes and identify where all those fraud dealings are happening. After that, you collect information and analyse and interview the…mostly the process owners. What else? Also you also examine the information that you've gathered to see if it's relevant or maybe you are gathering information that is not even relevant to your investigation. That's…then, obvious, after collecting and examining you compile a report. So a report, you use it to engage with those people that you were investigating or also maybe with managers so that they can actually explain why one, two, three's happening while there are controls in place to stop those kind of wrongful doings.

Another respondent indicated that the process starts with a project plan, followed by conducting interviews and gathering evidence, then the analysis and writing of the final report: *the team allocated to myself must do the project plan. A project plan it's how you are going to attend the investigation, the time allocated, the…you'll mention the interviews, fieldwork, the gathering of evidence, and then after whatever that you have obtained on the fieldwork, interviews must be analysed and have the report. After report writing it's…the report is presented to the client department.*

Three respondents indicated that they are not familiar with the processes of procurement fraud investigation. It is very difficult, if not impossible, for the CoT investigators who are not familiar with the processes to conduct a proper procurement fraud investigation that leads to a successful prosecution. CoT forensic investigators should familiarise themselves with the processes of procurement fraud investigation. It is, however, the responsibility of the CoT to provide in-service training or internal courses that will assist in elevating the knowledge of the processes of procurement fraud investigation.

4.4.4 Steps that could be implemented to assist in detecting and preventing future occurrences of procurement fraud

Effective procurement fraud detection and preventative methods will assist the CoT to establish or strengthen SCM internal controls, and to foster the necessary compliance by officials and service providers.

The respondents were asked to respond to the following question: *From your experience, name the steps that could be implemented to assist in detecting and preventing future occurrences of procurement fraud?*

There was consensus amongst all the participants that steps could be implemented to assist in the detection and prevention of future occurrences of procurement fraud, including: risk analysis, strengthening and strict internal controls, segregation of duties, implementation of hotlines and whistleblowing policies, training and workshops, lifestyle audits, independent oversight, automated systems and e-procurement. Interestingly, one respondent was of the opinion that detection will include monitoring the tender process, and prevention will include the rotation of SCM staff members and providing awareness campaigns to both employees and service providers: *Detection will be monitoring the tender process, will also…monitoring whether the service providers are rotated, monitoring if the service providers are vendor registered with your organisation, and monitoring the pattern in which the quotations are being requested. And the prevention part will be rotation of staff members and also providing awareness campaigns to both employees and service providers.*

In addition, the respondents also placed emphasis on the implementation of an automated system, that is, e-procurement and e-resources: *If I look at a[sic] automatic system, I would say that a [sic] automatic system should be implicated that's connected to, let's say, the SAP system, so that a weekly or a monthly or a quarterly report can be automatically composed to show the different buyers who were used which, how many times they used how many vendor , specific vendors, and how many vendors is [sic] on the book and is now used on a regular basis or not and that's the automatic system.*

Then a manual system will be to conducting [sic] audit on the process of certain procurement where you look at was the tender box locked? And you go through the process to see if everything was done according to… and then also for detecting if you look at how many incidents of procurement fraud happen [sic] in what phase of the procurement? And then that will automatically indicate a risk in that area.

For the effective detection and prevention of procurement fraud, the CoT should have refined software to track and log computer activities, and to signal a procurement fraud risk; for example*,* instances in which only one supplier is being appointed and there is no rotation of suppliers. Employees who are implicated should be prosecuted for procurement fraud, as this will serve as deterrent to others.

4.4.5 Procurement fraud red flags

Red flags are unusual activities that signal that something is out of the ordinary and may need to be looked at; this might lead to the investigation being instituted. In order to successfully deal with procurement fraud, CoT forensic investigators should familiarize themselves with procurement red flags.

The study respondents were asked to respond to the following question: *Briefly explain procurement fraud red flags and list examples?*

Eleven respondents explained red flags as unusual activities which are also warning signals for fraudulent activities. The same eleven respondents listed the following examples of red flags: officials accepting gifts from suppliers, lack of rotation, splitting of transactions by keeping them under thirty thousand rands, payments without invoices, missing pages on tender documents, unauthorised payments, change of lifestyle by officials, quotations with no cellphone numbers, deviations from SCM policies, unauthorized signatures, suppliers and officials being friends or family, unauthorized or unregistered vendors providing services and unusual payments.

One respondent was of the opinion that payments without invoices are a red flag: *Red flags will be payments without invoices. When you check payments you'll find out that one competitor is receiving large amounts of payments which are not justified. You'll find that there's one service provider doing multiple jobs for your company. You can find that they're not giving [INDISTINCT]. One company's doing something in IT, manufacturing, construction. Then you can see that there's something not going well there. You can check obviously authorisation, there's no proper authorisation of payments. You know who's supposed to authorise payments but you find that they're authorised by people who are not supposed to do so. Missing documents. When you look at the tender documents they're missing documents. I think that will be the red flags.*

Interestingly, three respondents expressed that change of lifestyle by officials is the most basic amongst the other red flags. One respondent indicated that *there are thousands of red flags. Lavish lifestyle within an employee who's got…which we cross-reference check their salary and according to their lifestyle audit their lifestyle audit doesn't correlate. That causes a red flag as well. And the list go [sic] on and on. Can I…should I list other ones?*

Being aware of procurement fraud red flags will reduce the larger scale of procurement fraud within the CoT municipality and it will lead to the successful investigation and prosecution of those involved.

4.4.6 Procedure of collecting and developing evidence during a procurement fraud investigation

It is common and best practice for the forensic investigator to design the procedures for how he/she will collect and develop evidence properly and legally. CoT forensic investigators should consider the basic procedures, such as interviewing witnesses and doing background checks to collect evidence.

The respondents were asked to respond to the following question: *From your experience, name the procedures that could be used to gather (collect) and develop evidence during a procurement fraud investigation?*

Thirteen respondents specified that the collection of information and documents, and the interviewing of witnesses are procedures to collect and develop evidence during a procurement fraud investigation. One respondent indicated that the following: *in terms of collecting evidence normally…because it's dependent on the client. You go to the client offices and you request for the different documents. You have a list of what you want. The policies…either you want the invoices, you want the quotations, you go to the various departments that are involved with each particular document and you get those ones. Normally we ask for originals and now that, like you said, there is SAPS* [*SP] sometimes you can sit with the guy who captured the transaction and see the transaction on the computer. You ask them to print it for you so you get them and then develop the evidence.*

One respondent suggested that the procedures will include interviewing the buyers and service providers, and collecting tender documents, policies and procedures: *I'll say procedures would be interviewing the buyers, interviewing the service providers, collection of documentation that was used during the tender process, and collection of policies and procedures that are being used during the tender process.*

It is worth noting that evidence should be collected by following an approved CoT investigation methodology and must adhere to the applicable legislation, such as law of evidence, otherwise it will be inadmissible in a court of law.

4.4.7 Critical information that must be collected during the investigation of procurement fraud

It is a common cause that any document, processes and stage of procurement will be critical to any procurement fraud investigation. Forensic investigators must collect any information related to the tender process and supply of goods and services. CoT forensic investigators should be familiar with this critical information that must be collected.

The respondents were asked to respond to the following question: *From your experience, name the critical information that must be collected during the investigation of procurement fraud?*

The resounding response from fourteen participants indicated that the following is critical information that must be collected during the investigation of procurement fraud: purchase orders, requisitions, appointment letters, contracts, payment history, SCM policies and procedures, tender documents, tender specifications, invoices, delivery notes, attendance registers of briefing sessions, CIPRO registration documents, vendor registration documents, tax certificates, MFMA and other related legislation.

One of the respondents further expressed a similar view by saying that appointment letters, requisitions, purchase orders, invoices, proof of payments and all relevant documents are critical to the investigation of procurement fraud: *Then let's start with the appointment of the service providers. Going back to the processes it's a long process. It depends how the scope is because if they say, no, we have ten people who are already appointed for this process…for this kind of procurement you go there, you obtain appointment letters. From appointment letters you go there and get a requisition from the services that the department or organisation wanted. Requisition, purchase order, and all relevant documentation, invoices from the service provider, and the proof of payments.*

Another respondent was of the opinion that the following is critical information to be collected during a procurement fraud investigation: vendor registration documentation, the requisition process, PO documents, invoices and even the delivery notes: *Again, that's difficult because it depends on what area you in…during the procurement you want the information but something that I recently saw that adds value to the investigation is the vendor registration documentation. Sometimes it would be the transactions that was allocated, the POs, the requisition process, PO documents. Sometimes it's the invoice and even the delivery notes. But, again, it depends on where…which stage in the procurement you are working where the irregularity allegedly took place.*

It is always important to collect as much information as possible to prove procurement fraud allegations. Most importantly, critical information such as contracts, quotations and payments history cannot be left behind.

4.4.8 Inhibiting factors that negatively impact forensics investigators' ability to optimally investigate procurement fraud

It is normal, particularly out of fear of being implicated in fraudulent activities, to resist cooperating and defy any instruction or query given by the investigators. These inhibiting factors impact on the investigators' ability to optimally investigate procurement fraud.

The respondents were asked to respond to the following question: *Do you experience any inhibiting factors that negatively impact your ability to optimally investigate procurement fraud? If affirmative, list these factors?*

The respondents unanimously agreed that the following are inhibiting factors that negatively impact their ability to optimally investigate procurement fraud: political interference, arrogance by officials, bullying tactics, non-cooperation, delay tactics, reluctance, refusal to write statements, unavailability or shortage of resources, inaccessibility to information, lack of IT and computer skills, and employees who resign before a case is finalised.

In this regard, one respondent indicated that it is quite frustrating to investigate a defiant, arrogant, uninterested, unwilling employee who always postpones investigation meetings: *Yes, a lot. I must say that it can be quite frustrating to try and do an investigating. One, you have unwilling parties. People are not willing to work with investigators because I think when they see you they see police cells. So they become defiant, they become arrogant, they become uninterested, unwilling, and then they usually like to go to occasion and due delays. Meeting postponements. They'll postpone meetings until you get frustrated. Lack of response to e-mails requesting for information or clarity. You will literally have to chase to get that evidence and people, though they know the truth, nobody wants to speak. They are in a court of silence. I'm telling you the truth. You can go and report me. It's like a court of silence and –.*

Moreover, the respondents highlighted that some CoT employees are reluctant to meet with investigators and to provide the required information: *Yes, reluctancy from some of the City of Tshwane employees to either meet with us for meetings, give us information which is required, it does inhibit doing our investigations on time because you can request certain documents, two months later you are still requesting them. You can request to meet a person, that person doesn't respond to you. So it does inhibit the progress of our investigations.*

The CoT should create a conducive environment for forensic investigators to conduct their investigations freely, without any hindrances. The CoT should also provide the necessary resources and training to its investigators. Management intervention will also be required to deal with defiant employees.

4.5 SUMMARY

This chapter provided a presentation and discussion of the quantitative data gathered from the semi-structured individual interviews of the study. The results of the survey were presented and the chapter discussion indicated the respondents' knowledge and views of the value of computer forensics in the investigation of procurement fraud within the CoT.

The participants’ responses were presented and discussed by means of emergent themes, so as to explore the outcomes of such interviews. An explanation of each theme provided the reader with a clear understanding of the themes and their subthemes.

In Chapter Five, the findings, recommendations and summary of the research are presented and discussed.

CHAPTER FIVE
FINDINGS, RECOMMENDATIONS AND CONCLUSION

5.1 INTRODUCTION

This chapter provides a summary of the findings, after which the interpretations made in Chapter Four are studied, and the relevant recommendations and conclusions are drawn. Recommendations are made, pertaining to the resultant findings from the themes presented in Chapter Four, regarding the value of computer forensics in the investigation of procurement fraud among FS forensic investigators within the GAR at the CoT. Should the recommendations made in this study be implemented, the value of computer forensics in the investigation of procurement fraud within the FS at the CoT could be realised; the underlying reasons why forensic investigators within the FS in the CoT cannot optimally investigate procurement fraud could be identified and efficiently acted upon; and the efficiency in computer forensics (of forensic investigators within the FS in the CoT) could be improved to successfully investigate incidents of procurement fraud. This study is significant, since the value of computer forensics in the investigation of procurement fraud within the FS at the CoT is identified and explored. This chapter further provides a summary of Chapters One to Five in conclusion of the chapter.

The aim of this study was to explore the value of computer forensics in the investigation of procurement fraud within the FS at the GAR at the CoT. In order to achieve the aim of this study, the following research questions were explored in line with the statement of the research problem and the aim of this study:

Firstly, to establish what the underlying reasons why forensic investigators within the FS in the CoT do not optimally investigate procurement fraud. Secondly, to ascertain how the efficiency in computer forensics, of forensic investigators within the FS in the CoT, could be improved to successfully investigate incidents of procurement fraud.
The researcher achieved the aim of this study and uncovered answers to the research questions by conducting a comprehensive literature review and conducting interviews

with fifteen FS investigators, particularly focusing on the research problem. This study is intended to empower the researcher and CoT forensic investigators with improved knowledge of the application of computer forensics during the investigation of procurement fraud.

The findings, recommendations and summary of the research are elaborated on in more detail below.

5.2 FINDINGS

The following findings were made based on the review of national and international literature supported by the empirical component of the study, that is, first-hand experiences received from respondents during the semi-structured interviews.

5.2.1 Research question 1: What is the value of computer forensics in the investigation of procurement fraud within the FS at the CoT?

The researcher established the following:

- The study was able to define the concepts “computer forensics” and “procurement fraud” and provide a breakdown of procurement fraud categories. It also clearly explained the objectives, methodologies, and types of computer forensic technologies. The four-step process of computer forensics is: identification, extraction or recovery, analysis, documentation and preservation of computer data and related materials in a manner that can be presented as evidence in a court of law and that will lead to the subsequent successful prosecution of the offenders.
- There is a definite need for computer forensics and it has become more apparent with the exponential increase in the number of cybercrimes.

- It is imperative and compulsory to apply computer forensics in any procurement fraud investigation in order to efficiently track down cyber criminals and solve complicated procurement fraud cases.
- Computer data is evidence that does not die and, if collected and properly preserved, it guarantees a conviction. CoT investigators who are not familiar with the steps to follow to preserve digital data tend to tamper with and destroy digital evidence, which leads to evidence rebuttal during criminal trials or disciplinary proceedings and casts doubt on the credibility of the evidence presented.
- Some CoT investigators are not familiar with the processes of procurement fraud investigation which makes it very difficult, or impossible, for them to conduct a proper procurement fraud investigation and lead to a successful prosecution.

5.2.2 Research question 2: What are the underlying reasons why forensic investigators within the FS in the CoT do not optimally utilise computer forensics to investigate procurement fraud?

The researcher established the following:

- The forensic investigators within the FS in the CoT lack the necessary computer skills to optimally investigate procurement fraud, as computer forensics requires extensive knowledge of computers and investigators should be uniquely qualified to conduct investigations involving computer software, data recovery and immense data analysis.
- Insufficient training contributed significantly to forensic investigators within the FS in the CoT not optimally utilising computer forensics to investigate procurement fraud.
- Political interference, arrogance by officials, bullying tactics, non-cooperation, delay tactics, reluctance, refusal to write statements, unavailability or shortage of resources, inaccessibility to information, lack of information and employees who resign before a case is finalised are the major contributing factors towards

forensic investigators within the FS in the CoT not optimally utilising computer forensics to investigate procurement fraud.

5.2.3 Research question 3: How can the efficiency in computer forensics, of forensic investigators within the FS in the CoT, be improved to successfully investigate incidents of procurement fraud?

The researcher established the following:

- To improve the FS forensic investigators' efficiency in computer forensics, proper training that is able to prepare and educate them to efficiently deal with computer forensic investigations must be provided.
- Computer training and procurement fraud skills development in the CoT should be a continuous process to develop and improve the efficiency of FS forensic investigators.
- Procurement fraud workshops must be provided to the FS forensic investigators timeously.

5.3 RECOMMENDATIONS

Based on what was discovered during the research, the following recommendations are made:

5.3.1 Research question 1: What is the value of computer forensics in the investigation of procurement fraud within the FS at the CoT?

- It is recommended that CoT forensic investigators acquire the necessary skills and essential training in computer forensics. This will improve CoT forensic investigators' knowledge and competence regarding the application and understanding of the value of computer forensics in the investigation of procurement fraud. This may also enhance CoT forensic investigators' investigative capacity through the facilitation of an improved procurement fraud prosecution rate.

- Computer forensic data must be properly collected and preserved following an approved CoT investigation methodology and must adhere to the applicable legislation, such as law of evidence. Failure to do so will result in the data being inadmissible in a court of law or attracting unnecessary disputes during trials or disciplinary proceedings.
- CoT forensic investigators should familiarise themselves with the processes of procurement fraud investigation. The CoT should provide in-service or internal training to assist in elevating the investigators' knowledge of the processes of procurement fraud investigations.

5.3.2 Research question 2: What are the underlying reasons why forensic investigators within the FS in the CoT cannot utilize computer forensics to optimally investigate procurement fraud?

- It is recommended that the CoT municipality develops a clear, consistent and sustainable education and skills enhancement programme involving computer forensics in order to ensure that investigators keep abreast of the evolution of a fast growing computer or digital world.
- CoT forensic investigators should constantly receive training on the application of computer forensics in forensic investigations and to improve their knowledge of the following areas:
    - Objectives of computer forensics
    - Four-step process of computer forensic investigation
    - Preservation of digital data
    - How to maintain chain of custody of computer forensic evidence.
- The CoT should create a conducive environment in which forensics investigators are able to conduct their investigations without any undue influence. The CoT should also provide the necessary resources and training to its investigators. Management intervention will also be required to deal with defiant employees.

5.3.3 Research question 3: How can the efficiency in computer forensics, of forensic investigators within the FS in the CoT, be improved to successfully investigate incidents of procurement fraud?

- It is recommended that in order for CoT forensic investigators to improve their efficiency in computer forensics, and to successfully investigate incidents of procurement fraud, training in the following areas must be provided:
    - Detection and prevention of procurement fraud
    - Identification of procurement red flags
    - Collection and developing of evidence during procurement fraud investigations
    - Critical information that must be collected during the investigation of procurement fraud

- The CoT should provide the necessary training and resources to the investigators. The CoT must make available the specialised software tools that required to analyse computer evidence and decrypt files, if so required by the forensic investigators.

5.4 CONCLUSION

Chapter One introduced the research by presenting the research problem. This was followed by an explanation of the research objectives and the research questions relevant to the study. A brief overview of how data was collected and analysed followed. All the relevant key terms were clarified, followed by a brief description of the methods taken to ensure the trustworthiness of the study, as well as the ethical framework within which the research was conducted.

Chapter Two dealt with the application of computer forensics in forensic investigation. The study established that computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. Four distinct steps in computer forensic investigations are identified: acquisition, identification, evaluation and presentation. Documentation is essential at all stages of handling and processing digital evidence. The goal of documentation is to establish the authenticity of the evidence and its admissibility.

Chapter Three dealt with an overview of the investigation of procurement fraud. The study established that procurement fraud is rife across the globe. This is particularly concerning in the CoT municipality as it has resulted in a loss of billions of Rands annually. However, with proper internal control and investigation, the reality of reducing procurement fraud risks in the CoT municipality is achievable. To ensure that forensic investigations are effective, CoT management should clearly set out its policies and procedures and give the forensic investigation division the authority and scope to do its job independently, without political influence. Forensic investigators must have a deep understanding of procurement fraud, focus on the risks, work closely with the external auditor and regulators, and create a control-conscious environment. Several computer software programs recommended in this study to aid CoT investigators with case management and reporting. Procurement fraud investigation will generally conclude with a formal written report of the investigation findings.

Chapter Four focused on the interpretation and discussion of the qualitative data collected from fifteen participants who were individually interviewed based on the survey. The participants' responses to these questions were then analysed by the researcher. The study revealed that the majority of the participants are familiar with computer forensics. Some have previously applied computer forensics in forensic investigation, even though most of them lack computer skills and require additional training in order to improve their ability to optimally investigate procurement fraud.

Chapter Five dealt with the findings and recommendations of the study. The research established that CoT forensic investigators lack the computer skills and knowledge to optimally investigate procurement fraud. Further training and greater provision of resources are recommended in order for the investigators to improve their ability to successfully deal with procurement fraud. The recommendations in this study could assist the CoT investigators in understanding the value of computer forensics in the investigation of procurement fraud. In addition, compliance with these recommendations could result in increased productivity and time-saving investigative methods and approaches, which will enhance the CoT investigators' ability to deal with procurement fraud.

LIST OF REFERENCES

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C. & Zimbelman, M.F. 2014. *Fraud examination*. 5th edition. Canada: Cengage learning.

Allen, J.M. & Sawhney, R. 2015. *Administration and management in criminal justice: A Service Quality Approach*. New Dehli: Sage.

American Bar Association. 2008. *State antitrust enforcement handbook*. United States of America: ABA.

Babbie, E. 2016. *The practice of social research.* 14th edition. Canada: Cengage Learning.

Bainbridge, D.I. 2008. *Introduction to information technology law*. 6th edition. Harlow: Pearson.

Barrow, L.M. & Rufo, R.A. 2014. *Police and profiling in the United States*. Boca Raton: Taylor & Francis.

Becker, R.F. & Dutelle, A.W. 2013. *Criminal investigation*. 4th edition. Burlington: Jones & Bartlett Learning.

Brown, C.L.T. 2010. *Computer evidence: collection and preservation*. 2nd edition. Boston: Cengage learning.

Carrier, B.D. 2006. *A hypothesis-based approach to digital forensic investigations*. *CERIAS Tech Report 2006-06*. Purdue University, Center for Education and Research in Information Assurance and Security. West Lafayette.

Cascarino, R.E. 2013. *Corporate fraud and internal control: A framework for prevention*. New Jersey: John Wiley & Sons.

Casey, E. 2011. *Digital evidence and computer crime: forensic science, computers and the internet*. 3rd edition. Waltham: Elsevier.

Champlain, J.J. 2003. *Auditing information systems*. 2nd edition. New Jersey: John Wiley & Sons.

City of Tshwane, Anti-fraud and Corruption Implementation Plan for the City of Tshwane, 2013. Pretoria: City of Tshwane Metropolitan Municipality.

City of Tshwane. 2012. *Enterprise risk management strategy*. Version No. ERM Strategy 002. Pretoria: City of Tshwane Metropolitan Municipality.

City of Tshwane, Forensic investigations. 2012. *Internal Audit report (2011 to 2012)*. Pretoria: City of Tshwane Metropolitan Municipality.

Coenen, T.L. 2008. *Essentials of corporate fraud*. New Jersey: John Wiley & Sons.

Cornick, M.S. 2014. *Using computers in the law office*. 7th edition. Clifton park. Cengage learning.

Corruption Watch. 2013. Dodgy procurement. From http://www.moneyweb.co.za/archive/r25bn-lost-every-year-to-dodgy-procurement/ (accessed 23 August 2015).

Creswell, J.W. 2012. *Qualitative inquiry and research design: choosing among five approaches*. 3rd edition. Thousand Oaks: Sage.

Creswell, J.W. 2014. *Research design. Qualitative, quantitative, and mixed methods approaches.* 4th edition. Thousand Oaks: Sage.

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

Denscombe, M. 2002(b). *The Good Research Guide for small-scale social research projects*. Philadelphia: Open University Press.

Denscombe, M. 2010. *Ground rules for social research: Guidelines for good practice*. New York: Open University Press.

De Vos, A.S., Strydom, H., Fouché, C.B. & Delport, C.S.L. 2007. *Research at grassroots for the social sciences and human services professions.* 3rd edition. Pretoria: Van Schaik.

EC-Council. 2010. *Computer forensics: Investigating network intrusions and cybercrime.* Clifton Park: Cengage learning.

Girard, J.E. 2015. *Criminalistics: Forensic science, crime, and terrorism*. 3rd edition. Burlington: Jones & Bartlett learning.

Golden, T.W., Skalak, S.L. & Clayton, M.M. 2011. *A guide to forensic accounting investigation.* New Jersey: John Wiley & Sons.

Goldmann, P.D. 2010. *Financial services: Anti-fraud risk and control*. New Jersey: John Wiley & Sons.

Grant, N. & Shaw, J. 2014. *Unified communications forensics: anatomy of common UC attacks*. Waltham. Elsevier

Hausman, K., Barrett, D. & Weiss, M. 2003. *Security+*. Indianapolis: Pearson IT Certification.

Holt, T.J, Bossler, A.M. & Seigfried-Spellar, K.C. 2015. *Cybercrime and digital forensics: An introduction*. New York: Routledge.

Johnson, T.A. 2005. *Forensic Computer Crime Investigation*. Boca Raton: Taylor & Francis.

Kanellis, P., Kiountouzis, E., Kolokotronics, N. & Martakos, D. 2006. *Digital Crime and Forensic Science in Cyberspace*. United States of America: Idea group.

Katz, N.A. 2012. *Detection and Reduction of Supply Chain Fraud*. London: Gower.

Kruse, W.G. & Heiser, J.G. 2002. *Computer forensics: Incident response essentials*. Indianapolis. Pearson education.

Leedy, P.D. & Ormrod, J.E. 2015. *Practical research: Planning and design.* 9th edition. Ohio: Merrill Prentice Hall.

Maras, M.H. 2015. *Computer forensics: Cybercriminals, laws and evidence*. 2nd edition. Sudbury: Jones & Bartlett learning.

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

Marcella (Jr), A.J. & Menendez, D. 2010. *Cyber forensics: A field manual for collecting, examining, and presenting evidence of computer crimes*. 2nd edition. Boca Raton: Taylor & Francis.

Marshall, C. & Rossman, G.B. 2014. *Designing qualitative research.* 6th edition. Thousand Oaks: Sage.

Maxfield, M.G. & Babbie, E. 2014. *Research methods for criminal justice and criminology*. 7th edition. Boston: Thomson-Wadsworth.

Maxwell, J.A. 2012. *Qualitative research design: An interactive approach*. 3rd edition. Thousand Oaks: Sage.

McCombie, S. & Warren, M. 2003. *Computer forensics: An issue of definition*. Proceedings of First Australian Computer, Network and Information Forensics Conference: Perth.

McMillan, E.J. 2006. *Policies and procedures to prevent fraud and embezzlement*. New Jersey: John Wiley & Sons.

Middleton, B. 2005. *Cyber Crime Investigator’s Field Guide*. Boca Raton: CRC Press.

Mouton, J. 2001. *How to succeed in your master’s and doctoral studies: A South African guide and resource book.* Pretoria: Van Schaik.

National Fraud Authority. (*Annual Fraud Indicator)* 2011. From http://www.gov.uk/ (accessed 29 January 2014).

Nelson, B., Philips, A. & Steuart, C. 2010. *Guide to computer forensics and investigation*. 3rd edition. USA: Cengage Learning.

Nelson, B., Philips, A. & Steuart, C. 2015. *Guide to computer forensics and investigation*. 5th edition. USA: Cengage Learning.

Newman, R.C. 2007. *Computer Forensics: Evidence Collection and Management*. Boca Raton: Taylor & Francis.

Nigel, L. & Samociuk, M. 2006. *Fraud and corruption: Prevention and Detection*. London: Gower.

Ochonma, E. 2015. *Procurement and Supply Chain Management: Emerging Concepts, Strategies and Challenges*. Bloomington: Author house.

O’Connor, P.D.T. & Kleyner, A. 2012. *Practical reliability engineering*. West Sussex: John Wiley & Sons.

Olsen, W.P. 2010. *The Anti-Corruption Handbook: How to protect your Business in the global marketplace*. New Jersey: John Wiley & Sons.

Oliver, P. 2013. *Writing your Thesis*. London: Sage.

Pachghare, V.K. 2015. *Cryptography and Information Security*. Delhi: PHL Learning.

Padgett, S. 2015. *Profiling the fraudster*. New Jersey: John Wiley & Sons.

Purpura, P.P. 2013. *Security and loss prevention: An introduction*. 6th edition. United States of America: Elsevier.

Report of the Auditor-General to the Gauteng Provincial Legislature and Council on the City of Tshwane Metropolitan Municipality. *Report on the Consolidated Financial*

Statement (2012). 14 December 2012. Auditor-General, Johannesburg, South Africa.

Reyes, A. & Wiley, J. 2007. *The best damn cybercrime and digital forensic book period: Your guide to digital information seizure, incident response, and computer forensics*. United States of America: Elsevier.

Sammes, T. & Jenkinson, B. 2013. *Forensic Computing: A practitioner's guide*. London: Springer-Verlag.

Sammons, J. 2012. *The basics of Digital forensics: The prime for getting started in digital forensics.* USA: Elsevier.

Schwartz, R. 2010. *Procurement fraud: Investigative techniques to help mitigate risk*. Swiss: Deloitte development LLC.

SCM Policy Amendment Report. 2011. City of Tshwane. From: http://www.tshwane.gov.za/Business/Tender%20Related%20Docs/SupplyChainPolicy.pdf (accessed 11 September 2013).

Shinder, D.L. & Tittel, E. 2002. *Scene of the Cybercrime: Computer forensic Handbook*. United States of America: Syngress.

Solomon, M.G., Barrett, D. & Broom, N. 2015. *Computer forensics JumpStart*. Indianapolis: Wiley.

Solomon, M.G., Rudolph, K., Tittel, E., Barrett, D. & Broom, N. 2011. *Computer forensics JumpStart*. 2nd edition. Indianapolis: Wiley.

South Africa. 2000. Preferential Procurement Policy Framework Act No. 5 of 2000. Pretoria: Government Printer.

South Africa. 2003. *Municipal Finance Management Act No. 56 of 2003*. Pretoria: Government Printer.

South Africa. National Treasury 2005. *Treasury Regulations for departments, trading entities, constitutional institutions and public entities.* Issued in terms of the Public Finance Management Act, 1999. March 2005.

South Africa. 2004. *Prevention and Combating of Corrupt Activities Act No. 12 of 2004.* Cape Town: Government Gazette No. 26311. *Special Investigation Unit.* 2013. Department of Justice and Constitutional Development. From: http://www.siu.org.za/ (accessed 11 August 2013).

Special Investigating Unit. 2010. *Training manual on procurement fraud*. East London: SIU

Special Investigating Unit. 2013. From: http://www.siu.org.za/who-we-are (accessed 31 January 2014).

Spollen, A.L. 1997. *Corporate Fraud: The danger from within*. Ireland: Oak Tree Press.

Stephenson, S. & Gilbert, K. 2013. *Investigating Computer-Related Crime*. 2nd edition. Boca Raton: Taylor & Francis.

Supply Chain Management. *Vendor Registration.* 2009. City of Tshwane. From: http://www.tshwane.gov.za/AboutTshwane/CityManagement/CityDepartments/Financial%20Services/Pages/Supply-Chain-Management.aspx (accessed 11 September 2013).

Tewari, R.K., Sastry, P.K. & Ravikumar, K.V. 2002. *Computer crime and computer Forensics*. India: Select.

University of South Africa. 2007. *Policy on Research Ethics*. Florida: UNISA.

Vacca, J.R. 2011. *Computer forensics: computer crime scene investigation.* Massachusetts: Charles River Media.

Vanasco, R.R. 1997. *Fraud Auditing: An international perspective.* California: Cat.

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

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

Welman, J.C. & Kruger, S.J. 2002. *Research methodology for the business and administrative sciences.* 2nd edition. Cape Town: Oxford University Press.

Welman, J.C., Kruger, S.J. & Mitchell, B. 2005. *Research methodology.* 3rd edition. Cape Town: Oxford University Press Southern Africa.

Wells, V.D. 2011. *Principles of fraud examination*. New Jersey: John Wiley & Sons.

West, H. 1987. *Fraud: The growing Industry*. London: Professional publishing limited.

Wilding, E. 1997. *Computer evidence: a forensic investigations handbook*. London. Sweet & Maxwell.

Wiles, J. 2007. *Techno security's guide to e-discovery and digital forensics*. USA: Elsevier.

ANNEXURE A

INTERVIEW SCHEDULE

EXPLORING THE VALUE OF COMPUTER FORENSICS IN THE INVESTIGATION OF PROCUREMENT FRAUD

1. BACKGROUND INFORMATION

1.1 What is your current position at the CoT Forensic Services?

1.2 What is your highest tertiary qualification?

1.3 How many years of forensic investigation experience do you have at the CoT Forensic Services?

1.4 How many computer forensics investigations have you conducted in the past 12 months, as part of an investigation to prove procurement fraud?

1.5 Have you undergone any formal training in computer forensics, cyber forensics, digital forensics or procurement fraud investigation? If affirmative, indicate the relevant training courses completed?

2. THE APPLICATION OF COMPUTER FORENSICS IN FORENSIC INVESTIGATION

2.1 What is your understanding of the term ‘computer forensics’?

2.2 According to you, what are the objectives of computer forensics?

2.3 Are you familiar with the four-step process of computer forensic investigation? If affirmative, briefly name these steps. If not, motivate why not?

2.4 Have you previously applied computer forensics in procurement fraud investigations? If affirmative, did it add value to the investigation? How? If not, why not?

2.5 Are you conversant (familiar) with the steps that a computer forensic investigator should follow to preserve digital data for future computer forensic examination? If affirmative, briefly list these steps. If not, motivate why not?

2.6 Are you familiar with how to maintain the chain of custody of evidence seized during a computer forensic investigation? If affirmative, briefly indicate how you maintained the chain of custody? If not, motivate why not?

2.7 According to you, what are the basic qualities that a computer forensic investigator should have?

2.8 In your opinion, have you received sufficient training to confidently conduct effective computer forensic investigations? If not, how could your efficiency as a computer forensic investigator be improved?

3. AN OVERVIEW OF THE INVESTIGATION OF PROCUREMENT FRAUD

3.1 What is your understanding of the term ‘procurement fraud’?

3.2 Are you familiar with the different types of procurement fraud? Briefly list these types of procurement fraud?

3.3 According to you, what are the processes of procurement fraud investigation? Briefly name these requirements?

3.4 From your experience, name the steps that could be implemented to assist in detecting and preventing future occurrences of procurement fraud?

3.5 Briefly explain procurement fraud red flags and list examples?

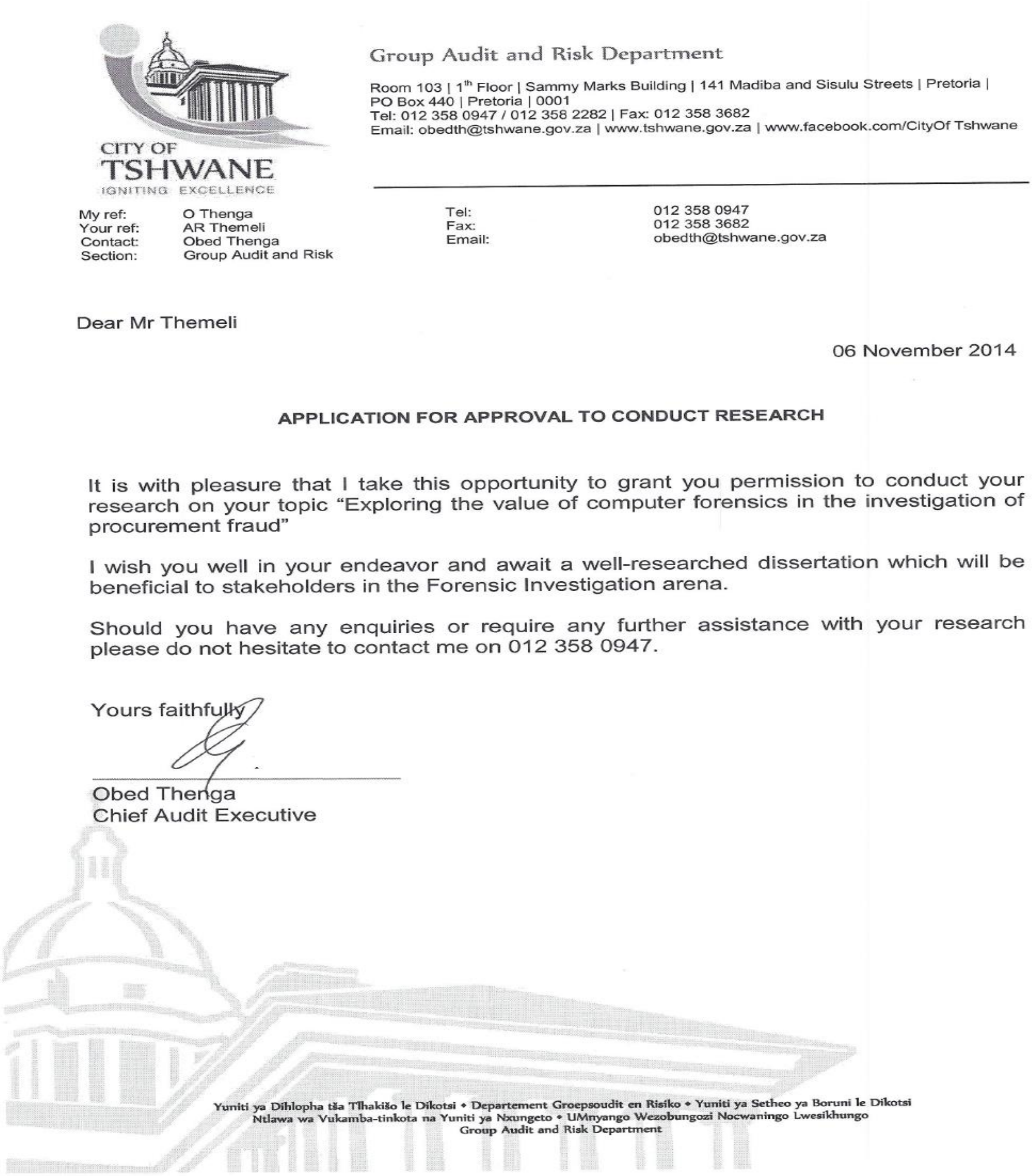
3.6 From your experience, name the procedures that could be used to gather (collect) and develop evidence during a procurement fraud investigation?

3.7 From your experience, name the critical information that must be collected during the investigation of procurement fraud?

3.8 Do you experience any inhibiting factors that negatively impact your ability to optimally investigate procurement fraud? If affirmative, list these factors?

ANNEXURE B

APPROVAL TO CONDUCT RESEARCH: CITY OF TSHWANE



CITY OF
TSHWANE
IGNITING EXCELLENCE

Group Audit and Risk Department

Room 103 | 1th Floor | Sammy Marks Building | 141 Madiba and Sisulu Streets | Pretoria |
PO Box 440 | Pretoria | 0001
Tel: 012 358 0947 / 012 358 2282 | Fax: 012 358 3682
Email: obedth@tshwane.gov.za | www.tshwane.gov.za | www.facebook.com/CityOf Tshwane

My ref:	O Thenga	Tel:	012 358 0947
Your ref:	AR Themeli	Fax:	012 358 3682
Contact:	Obed Thenga	Email:	obedth@tshwane.gov.za
Section:	Group Audit and Risk		

Dear Mr Themeli

06 November 2014

APPLICATION FOR APPROVAL TO CONDUCT RESEARCH

It is with pleasure that I take this opportunity to grant you permission to conduct your research on your topic "Exploring the value of computer forensics in the investigation of procurement fraud"

I wish you well in your endeavor and await a well-researched dissertation which will be beneficial to stakeholders in the Forensic Investigation arena.

Should you have any enquiries or require any further assistance with your research please do not hesitate to contact me on 012 358 0947.

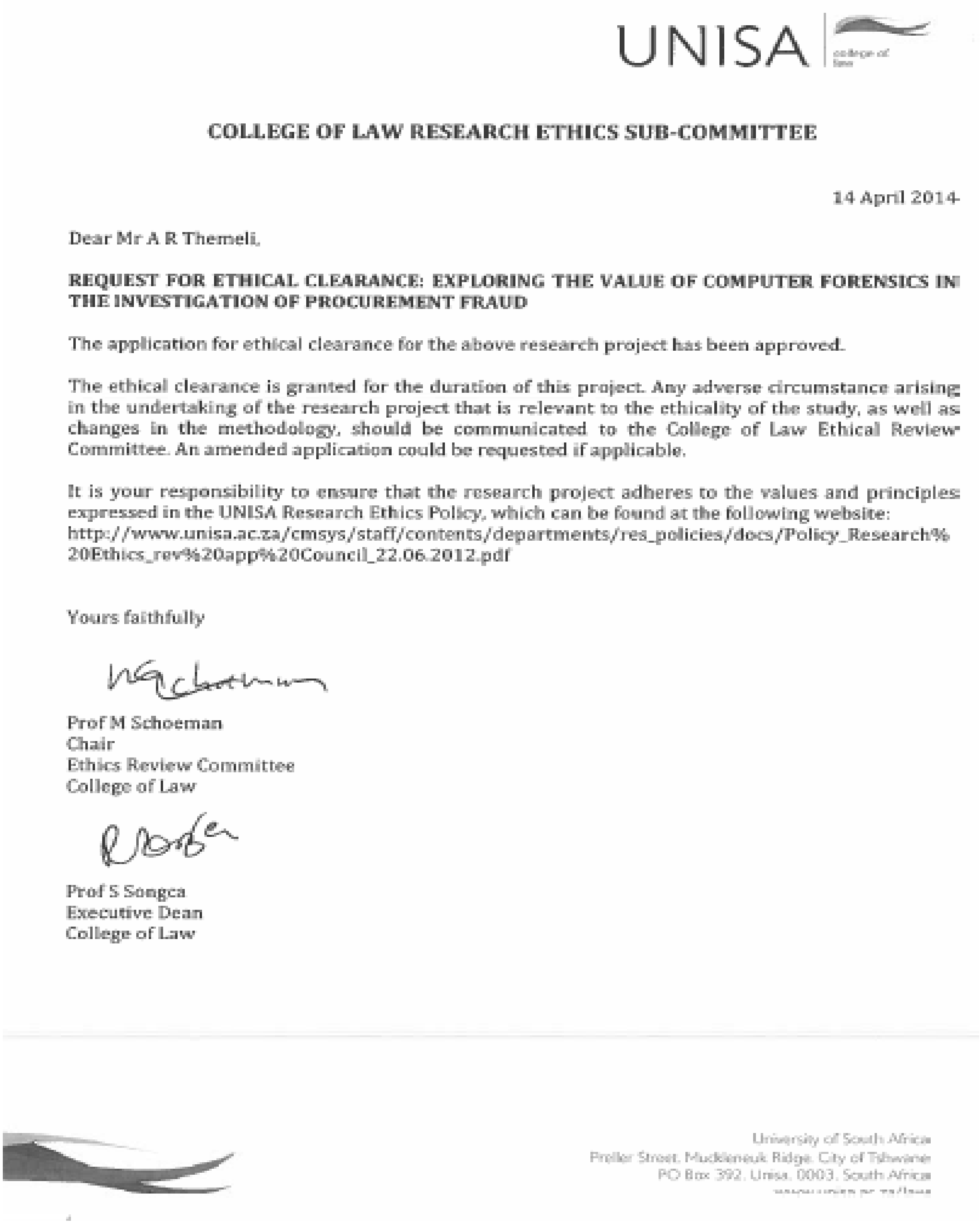
Yours faithfully

Obed Thenga
Chief Audit Executive

Yuniti ya Dihlopha tša Tlhakišo le Dikotsi • Departement Groepsoudit en Risiko • Yuniti ya Setheo ya Boruni le Dikotsi
Ntlawa wa Vukamba-tinkota na Yuniti ya Nxungeto • UMnyango Wezobungozi Nocwaningo Lwesikhungo
Group Audit and Risk Department

ANNEXURE C

ETHICAL CLEARANCE: UNIVERSITY OF SOUTH AFRICA



UNISA
college of law

COLLEGE OF LAW RESEARCH ETHICS SUB-COMMITTEE

14 April 2014

Dear Mr A R Themeli,

REQUEST FOR ETHICAL CLEARANCE: EXPLORING THE VALUE OF COMPUTER FORENSICS IN THE INVESTIGATION OF PROCUREMENT FRAUD

The application for ethical clearance for the above research project has been approved.

The ethical clearance is granted for the duration of this project. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated to the College of Law Ethical Review Committee. An amended application could be requested if applicable.

It is your responsibility to ensure that the research project adheres to the values and principles expressed in the UNISA Research Ethics Policy, which can be found at the following website:
http://www.unisa.ac.za/cmsys/staff/contents/departments/res_policies/docs/Policy_Research%20Ethics_rev%20app%20Council_22.06.2012.pdf

Yours faithfully

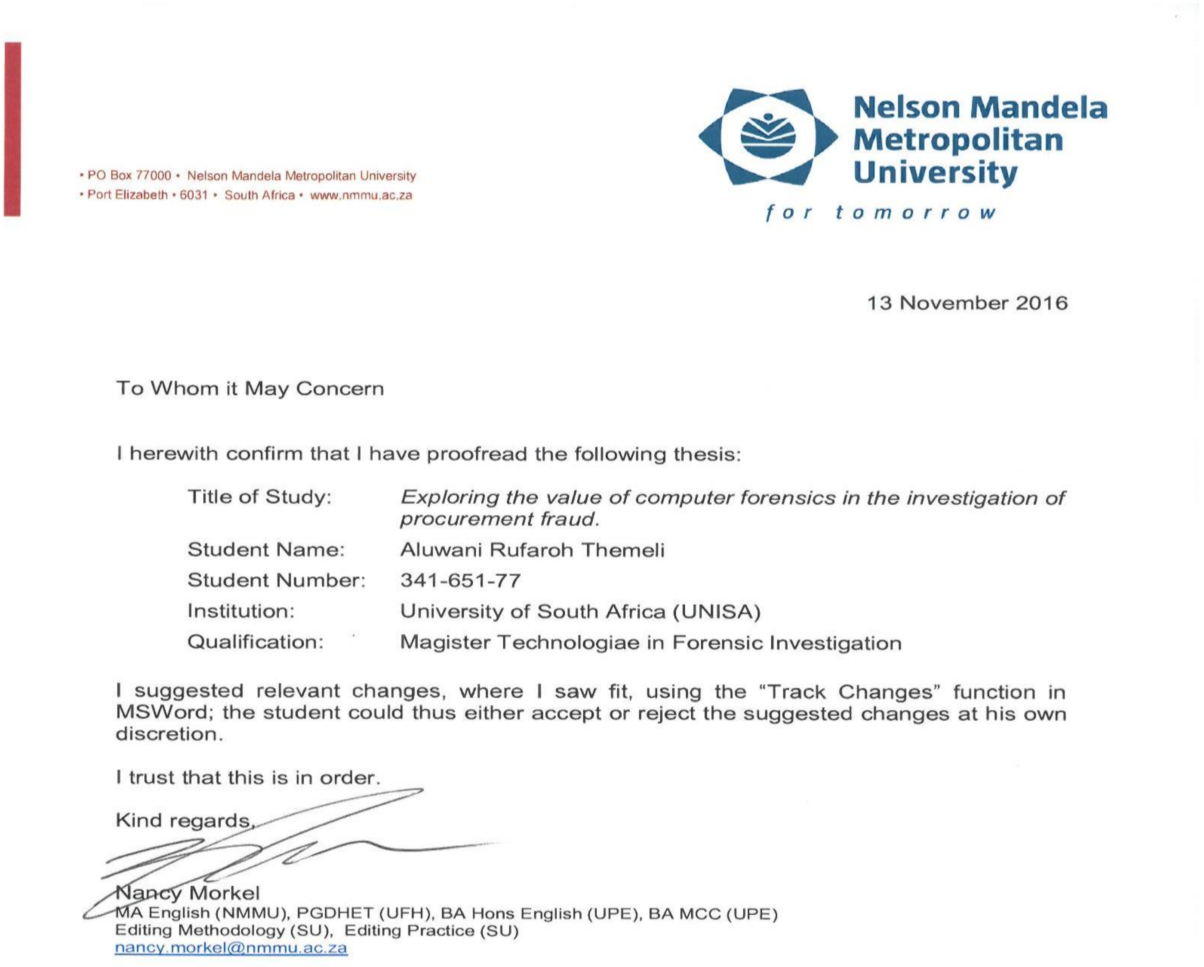
Prof M Schoeman
Chair
Ethics Review Committee
College of Law

Prof S Songca
Executive Dean
College of Law

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392, Unisa, 0003, South Africa
www.unisa.ac.za/law

ANNEXURE D

EDITING CERTIFICATE



• PO Box 77000 • Nelson Mandela Metropolitan University
• Port Elizabeth • 6031 • South Africa • www.nmmu.ac.za

Nelson Mandela
Metropolitan
University
for tomorrow

13 November 2016

To Whom it May Concern

I herewith confirm that I have proofread the following thesis:

Title of Study:	*Exploring the value of computer forensics in the investigation of procurement fraud.*
Student Name:	Aluwani Rufaroh Themeli
Student Number:	341-651-77
Institution:	University of South Africa (UNISA)
Qualification:	Magister Technologiae in Forensic Investigation

I suggested relevant changes, where I saw fit, using the "Track Changes" function in MSWord; the student could thus either accept or reject the suggested changes at his own discretion.

I trust that this is in order.

Kind regards,

Nancy Morkel
MA English (NMMU), PGDHET (UFH), BA Hons English (UPE), BA MCC (UPE)
Editing Methodology (SU), Editing Practice (SU)
nancy.morkel@nmmu.ac.za