PROCEDURES FOR SEARCHING EVIDENCE IN THE INVESTIGATION OF COMPUTER-RELATED CRIME IN BULAWAYO, ZIMBABWE

by

NJABULO NCUBE

Submitted in partial fulfilment of the preliminary for the

MAGISTER TECHNOLOGIAE

in the subject

FORENSIC INVESTIGATION

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: S. M. MANAMELA

November 2015

ABSTRACT

The continued advancement in myriad technological, societal and legal issues has affected the investigation of computer aided crimes. The investigators are confronted with tremendous impediments as the computer aided and traditional crime scenes differ. The study sought to analyse the procedures for searching evidence in the investigation of computer-related crime with the intention to improve admissibility of such evidence.

The researcher employed empirical design to reach conclusions based upon evidence collected from observations and real life experiences. This aided the researcher to obtain information through face-to-face interviews. The study was qualitative in approach as it consisted of a set of interpretive and material practices that make the real social world visible.

The training curriculum for investigators should include aspects of computer-related crime investigation, search and seizure of computer evidence. Search and collection of computer-related evidence should be done preferably by qualified forensic experts, so that evidence is accepted in court.

Key Terms:

Criminal Investigation; Forensic Investigation; Computer forensics; Computer-related crime; Search; Search warrant; Evidence; chain of evidence;

DECLARATION

I, **Njabulo Ncube,** declare that "**Procedures for searching evidence in the investigation of computer-related crime in Bulawayo, Zimbabwe**" 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.

(N Ncube)

SIGNATURE DATE

ACKNOWLEDGEMENTS

Humanly speaking, the writing of this dissertation was an academic challenge that seemed impossible. But with God everything is possible.

I express my sense of gratitude in acknowledging my supervisor Mr. M.S. Manamela for his excellent guidance, caring, patience, support and encouragement. He provided me a conducive atmosphere for doing this research.

I also acknowledge the Commissioner General of the Zimbabwe Republic Police (ZRP) for the opportunity granted to me to conduct this research in their environment. My profound gratitude also goes to the participants for their cooperation during this research.

A special acknowledgement goes to my loving wife Siduduzile who stood by me and was always cheering me up through good and bad times; and my children Thando, Bongani and Unathi for believing in me, and their unwavering encouragement during this research.

I would like to thank my colleague Doctor Whitehead Zikhali who was willing to help and give guidance and suggestions. I also express my sense of gratitude to Nhlanhla Sibanda, an English and Communication Studies lecturer at the Zimbabwe Open University, for editing my dissertation.

I would not have done any justice if I do not acknowledge my dear sister Tokozile Marah. She identified my potential, inspired and motivated me.

LIST OF ABBREVIATIONS

AC	Assistant Commissioner
APCO	Association of Chief Police Officers
ATM	Automated Transaction Machine
BIOS	Basic Input Output System
BSI	British Standards Institution
CBI	Central Bureau Investigation
CD	Compact Disk
CD-ROMS	Compact Disk-Read-Only Memory
CFFTPM	Computer Forensics Field Triage Process Model
CFTT	Computer Forensic Tool Testing
CID	Criminal Investigation Department
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
DEB	Digital Evidence Bag
DEG	Digital Evidence Group
DFRWS	Digital Forensics Research Workshop
DI	Detective Inspector
DoS	Disk Operating System
DVD	Digital Versatile Disks
EDIP	Enhanced Digital Investigation Process Model
FBI	Federal Bureau of Investigation
FTK	Forensic Tool Kit
FSL	Forensic Science Laboratory
GFS	Group Forensic Services
IDIP	Integrated Digital Investigation Process
IDS	Intruder Detection System

IP	Internet Protocol address
ISP	Internet Service Provider
ISFS	Information Security and Forensics Society
LAN	Local Area Network
MD5	Message Digest 5
NIST	National Instate of Standards and Technology
PC	Personal Computer
PDAs	Personal Digital Assistant
PDF	Portable Document Format
PPA	Privacy Protection Act
PUC	Provincial Updating Centre
RAM	Random Access Memory
SHAH 1	Secure Hash Algorithm 1
SWDGE	Scientific Working Group for Digital Evidence
UNDP	United Nations Development Programme
UK	United Kingdom
US	United States
USA	United States of America
USB	Universal Serial Bus
ZIMRA	Zimbabwe Revenue Authority
ZRP	Zimbabwe Republic Police

TABLE OF CONTENTS **PAGES**

CHAPTER 1: GENERAL ORIENTATION

1.1 INTRODUCTION

Computer-related crime is a new phenomenon in Zimbabwe. Alexandrou (2011:1) defines computer related crime as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation or prosecution. Kunz and Wilson (2004:7) acknowledge the foregoing definition and further assert that computer related crimes are offences committed in a technological environment. The continued advancement in myriad technological, societal and legal issues has affected the investigation of computer aided crimes peculiarly to procedures for searching of evidence. The Zimbabwe Criminal Law (Codification and Reform), Act 23 of 2004 was promulgated to address crime, unfortunately the legislative enactment does not mention computer aided crimes as direct crime and lags behind in addressing the actual practice of computer-based crime much more than in other crimes.

Goodman (1997:468) posits that computer-related crime covers wide range of offences that unanimity has been an elusive goal. On the other hand, Mobbs (2003:1) is of the opinion that computer-related crime is an often used term that has a very vague meaning. The majority of computer-related crimes amongst other things were viewed as conventional crimes aided by the use of computers. Computer-related crime is growing rapidly and constitutes a new confrontation to all levels in how to prevent, investigate, and prosecute it (Kunz and Wilson, 2004:10). During the commemorations to mark World Telecommunications Day under the theme of "Promoting Global Cyber security", the Zimbabwean government, Transport and Communication Minister Christopher Mushowe acknowledges the foregoing when he mentions that laws aided for the enforcement of computer-related crimes are outdated (Zimbabwe Herald, 2009:11).

In view of the prevalence of computer-related crimes, there is an emerging need for Law enforcement Officers to appreciate how these crimes vary from the traditional crime as this will provide them with insights for computer-related investigative strategies.

1.2 STATEMENT OF THE PROBLEM

The inadequacy of the Chapter 9 (23) in the Zimbabwe Criminal Law (Codification and Reform) Act 23 of 2004 that addresses computer-related crime and the deficiency in the manner in which searching procedures are executed, make it difficult for investigating officers at Bulawayo Metropolitan Criminal Investigation Department to respond to computer-aided crime adequately. During pre-research discussions, it became clear to the researcher that investigating officers at Bulawayo Criminal Investigation Department were confronted with tremendous impediments. This is because computer-aided crime scene differs from traditional crime scene and there is no optimal approach to strategies used to search for evidence. According to the Criminal Investigation Department (CID) spokesperson, cyber-crime is on the increase due to the esoteric nature of this crime and there are limited prosecutions with diminished convictions (Bulawayo 24 News, 2012:4).

During the preliminary investigations, the researcher, a former Chief Superintendent in the Zimbabwe Republic Police, had a discussion with Assistant Commissioner (AC) Nkomo, the current Regional Coordinator of Matabeleland Provinces; and Detective Inspector (DI) Alford, the team leader of cybercrime Investigations at Bulawayo Criminal Investigations department. They informed the researcher of the deficiencies they had observed in the manner in which investigators executed procedures for searching evidence during the investigation of computer-related crime. Assistant Commissioner made the observations as she was perusing dockets during her annual scheduled inspections.

Their experience was corroborated by the statistics enshrined in the Bulawayo Metropolitan Service Plan document (2012) covering the period extending from January, 2010 to December 2011. The Metropolitan Service Plan (2012) document depicted 42% of computer-related cases were either, declined to be prosecuted, withdrawn on or before plea or persons acquitted. This was due to investigating officers who lacked understanding of the fundamental principles of searching set forth under the traditional legal concepts applied to search and seizure of computer-related crime evidence (Feltoe, 2009:19). There were three Criminal Investigators seconded to Bulawayo Tredgold Magistrate Court as Police Public Prosecutors having done Prosecutor's course and amongst other cases prosecuted computer-related crime. The Police Public Prosecutors stated that they were the source of the foregoing statistics. They had observed during the same period under review limitations in the fashion in which the investigators discharged the procedures for searching evidence in computer-related matters leading to the inadmissibility of such evidence. Any evidence collected in violation of the prescribed procedure is considered to be "fruit of the poisonous tree," and will not be admissible in court (Johnson, 2008:150). Furthermore, any evidence identified and gathered as a result of the initial inadmissible evidence will also be held to be inadmissible in court. Johnson (2008:146) further highlighted that such evidence is excluded for other reasons, such as violations related to conducting any search.

The researcher was of the opinion that failure to adhere to the correct procedures in searching for evidence during investigation of computer-related crime will destroy valuable evidence and/or cause greater losses to evidence that will contribute immensely in the convictions rate. As this problem was more prevalent in the day-to- day work of the Bulawayo Metropolitan Criminal Investigation Department Investigating Officers, the researcher identified the need for this study. The intention was to contribute to streamlining and strengthening the manner in which procedures are followed when searching evidence during investigation of computer-related crime. The researcher looked at the national and international best practices related to fundamental principles,

rules, exceptions, applicability and compatibility of search of evidence in computer crime as outlined in the guidelines mentioned under Zimbabwean Criminal Procedure and Evidence Act 14 of 2004. The study concluded a number of recommendations formulated on the basis of the findings. This enriched literature in this area and provided guidelines to Bulawayo Metropolitan Criminal Investigation Department Investigating Officers.

1.3 AIM OF THE STUDY

According to Welman, Kruger and Mitchell (2005:2), the aim of research is to obtain scientific knowledge by means of various objective methods and procedures. Whereas, Shuttleworth (2008:1) states that the ultimate aims of research is to generate measurable and testable data, gradually adding to the accumulation of knowledge.

Therefore, the aim of this research was to analyse the manner in which investigators executed the procedures for searching of evidence during investigation of computer-related crime with the intention to improve admissibility of such evidence.

1.4 PURPOSE OF THE RESEARCH

It is Denscombe (2002:25)'s assertion that research should be influenced by a substantial motivation; otherwise it will be futile to spend money and time on an unsubstantial investigation. The purpose statement should depict the hub and the path of the research explicitly and endeavour to avail a standard in which evaluation of the research is based.

As guided by Denscombe (2002:25-27), the researcher opted for the *infra* purposes of this research:

(a)To evaluate the manner in which the Investigation Officers execute searching procedures during investigation of computer related crime with the aim of establishing the strengths and weak points in the process and consider how searching techniques can be improved.

(b)The researcher wants to explore national and international sources in order to find new information on procedures followed in searching for evidence during investigation of

computer related crime and use the information to strengthen the established weak points.

(c)The researcher wants to use the acquired research knowledge to develop good practices and guidelines that will be recommended to Bulawayo Metropolitan Criminal Investigation Department Investigating Officers.

1.5 RESEARCH QUESTIONS

According to Paulsen (2010:1), research questions make explicit exactly what you want to investigate and George (2011:1), mentions that a research question expresses what the research project aims to find out. It gives the structure and focus necessary to get meaningful and useful results.

This study will seek to find answers to the following questions, which were set to guide the whole study:

- What does computer-related crime entail?
- How are searching procedures executed during investigation of computer-related crime for evidence to be admissible in court?

1.6 KEY THEORETICAL CONCEPTS

Researchers define terms so that readers can understand their unambiguous meaning. Creswell (2003:161) explains that definitions of key concepts enable individuals to understand terms that are not common language. Defining terms adds precision to a research study and ostensibly strips the multiplicity of meaning from words in the interest of precision (Creswell, 2003:161). The key concepts that are relevant to this study are defined *infra.*

1.6.1 Criminal Investigation

Gunter and Hertig (2005:1) define investigation as a systematic fact finding and reporting process. It is derived from the Latin word *vestigere,* to “track or trace” (Bennett & Hess, 2004: 4).

1.6.2 Forensic Investigation

According to Lytle (2008:1), forensic investigation is a practice within the confines of law for constructing evidence for the purpose of proving true facts that are to be presented in a competent court of law.

1.6.3 Computer Forensics

Solomon and Lattimore (2008:1), define computer forensic as the process to determine and relate extracted information and digital evidence to establish factual information for judicial review.

1.6.4 Computer-related crime

Alexandrou (2011:1), define computer-related crime as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigations, or prosecution.

1.6.5 Search

According to Loginsky (2011:52), search is a procedure used in many common law and civil legal systems whereby police or other authorities and agents who suspect that a crime has been committed conduct a search of a person's property with the intention of confiscating any relevant evidence to be used in the court of law.

1.6.6 Search warrant

According to Collins (2007:2), search warrant is a written document that represents judicial authorization for peace officers to enter and search a specific place for items and to seize those items that are evidence to the offence, if they are found.

1.6.7 Evidence

According to Chawki (2004:1), evidence is" information, whether in the form of personal testimony, the language of a document, or production of material objects, that is given in legal investigation, to establish the fact or point in question".

1.7 RESEARCH DESIGN AND APPROACH

1.7.1 Research design

According to Singh (2006:77), research design is a mapping strategy. It is an essential statement of the object of the inquiry and the strategy for collecting the evidences, analysing the evidences and reporting the findings. The researcher employed empirical design in which Oates (2012:2) and Singh (2006:9) describe as any conclusion drawn based upon hard evidence gathered from information collected from real life experiences or observations. On the other hand, Mouton (2001:53) affirms that empirical research analyses existing data and addresses a real-life problem. The rationale of using this design was for the researcher to obtain factual information from the participants by conducting face-to-face interviews. The researcher also analyzed closed reported computer-related cases and reviewed literature in addressing the topic.

1.7.2 Research approach

The study is qualitative in approach and in nature because it covers an array of interpretive techniques, which seek to describe, decode, translate, and otherwise come to terms with the meaning of naturally occurring phenomena in the social world (Welman et al., 2005:188). Furthermore, Hagan (2003:19) describes qualitative research as sensitizing ideas or terms that enhance our understanding. Van As and Van Schalkwyk

(2000:176), further mention that qualitative researches describe events and persons scientifically without using numerical data. In summary, the researcher used literature and had to seek information in the field through case docket analysis and interviews as instruments for collecting data.

1.8 TARGET POPULATION AND SAMPLING

According to Welman et al. (2005:52), population encompasses the total collection of all units about which the researcher wishes to make specific conclusions. It is the entire mass of observations, which is the parent group from which a sample is formed (Singh, 2006:82). In this research, the population referred to is the entire investigators in the Criminal Investigation Department in Zimbabwe who investigated cybercrime and all the Police Public Prosecutors who prosecuted cybercrime. The practical limitation such as cost, time and other factors which are usually operative in the situation stood in the way of studying the total population. The researcher therefore decided to work with a target population.

According to Creswell (2003:177), target population is the population to which the researcher would ideally like to generalize his results. The target population for this study was cybercrime investigators at Bulawayo Metropolitan Criminal Investigation Department Policing area and the Police Public Prosecutors based at the Bulawayo Metropolitan Tredgold and Western Commonage Magistrates Courts. The researcher resides at the Bulawayo Metropolitan, therefore this saved time and costs as this research was not sponsored. The Bulawayo Metropolitan is located in the Southern part of Zimbabwe known as Matabeleland.

Non-probability sampling was used in the study. According to Oates (2012: 96), and Singh (2006: 86), non-probability is used when the researcher believes it is not feasible or necessary to have a representative sample. The population was purposively selected from a target of ten Criminal Investigation Department stations in Bulawayo Metropolitan Criminal Investigation Department Policing area who served the following three districts, namely, Bulawayo West, Bulawayo Central and Bulawayo Suburban. The reasons for purposively selecting the mentioned Policing area as guided by Oates (2012:98), were as

follows; all investigating officers in this department investigated the same type of computer-related crime, received same training, uniform in structure, composition and were logically homogeneous. To be regarded as a cybercrime investigator in Zimbabwe, the investigating officers must meet specific thresholds, defined investigation capabilities and experience. Therefore, there were twenty-seven (27) investigators in the Bulawayo Metropolitan Criminal Investigation Department Policing area that investigated computer-related crime and the researcher decided to include all the twenty seven (27) investigators. The researcher also purposefully selected three (3) Commanding Officers responsible for units in the Bulawayo Metropolitan Criminal Investigation Department Policing area bringing the total to thirty (30) participants referred to as sample A.

There were only three (3) serving Police Public Prosecutors in Bulawayo Metropolitan Criminal Investigation department of which two were seconded to Tredgold Magistrate Courts and one to Western Commonage Courts respectively. The three Police Public Prosecutors received similar Prosecutor's training and prosecuted similar cases and were selected to undergo Prosecutor training using similar criteria. The researcher interviewed the three serving Police Public Prosecutors in the Bulawayo Metropolitan who were selected through purposive sampling based entirely on the judgement of the researcher, in that a sample is composed of elements that contain the most characteristics representative or typical attributes of the population (Welman et al., 2005:69). The three (3) Police Public Prosecutors are referred to as sample B.

According to Oates (2012:98), purposive sampling is selected by non-probability but for some particular reason or for some characteristics that it possesses, and for this reason the three Police Public Prosecutors were well suited to be selected through purposive sampling as the sample "B" because they were likely to produce valuable data to meet the purpose of the research.

1.9 DATA COLLECTION

According to Singh (2006:212), data refers to an elementary description of things, events, activities and transactions that are recorded, classified, stored and used as a basis for inference or reckonings. Oates (2012: 36) describes data generation methods as the means by which empirical data or evidence is produced. The researcher was interested in qualitative data which, according to Oates (2012:36), is all types of data produced in language through the minds of participants or interviews. The researcher collected primary data. According to Welman et al. (2005:149), primary data consists of written or oral accounts of a direct witness to or a participant in an event, or an audiotape, videotape or photographical recording of it.

The researcher used three data generation methods, thus literature, interviews and case docket analysis. The use of more than one data collection method to corroborate findings and enhance their validity is referred to as triangulation and it gives the researcher multiple modes of attack on the research questions (Creswell, 2003:248). According to Bailey-Beckett and Turner (2009), triangulation is the application and combination of more than one research perspective in the study of the same phenomenon. Jakob (2001) and Golafshani (2003: 597) reiterate that by combining multiple observers, theories, methods, and empirical materials, researchers can hope to overcome the weakness or intrinsic biases. This includes the problems that come from single-method, single-observer and single-theory studies.

1.9.1 Review of Related Literature

According to Singh (2006:37), effective research is based upon past knowledge to eliminate replication of what has been done and synthesize the available knowledge of the field in a unique way to provide the rationale for the study. It provides a frame work for establishing the importance of the study as well as a benchmark for comparing the results of a study with other findings (Creswell, 2006:31). The researcher visited Zimbabwe Republic Police Staff College library, the three libraries in Bulawayo and Bulawayo Provincial Updating Centre (PUC) to locate books on the same topic as that of

the present study. The researcher collected information on books about computer-related crime, search and seizure, judicial precedence's, journals, manuals, newspapers, magazines and the Internet. Criminal justice websites were also explored for any material on the same topic and information that described the researcher's questions and objectives.

Welman et al. (2005:40), describe the identification of key words or search terms as the most important part of literature search and discuss the researcher's ideas as widely as possible. In order to ensure that all literature were treated the same and obtained greater numbers of sources, the researcher divided the research topic into the *infra* concepts "forensic investigation", "criminal investigation", "evidence", "computer-related crime", "computer forensics", search and seizure" and "search warrant". The foregoing sources were searched for information that covered and provided relevant answers to the research questions.

The contents and the quotes were analysed by comparing data to establish where the authors concurred and where their views and findings differed. In summary, all information collected was combined, integrated and interpreted to find any correlation to each other.

1.9.2 Interviews

According to Oates (2012:186), an interview is a particular kind of conversation between people and it has a set of assumptions that do not apply to normal conversations.

The researcher used structured interviews for the twenty-seven (27) investigators and three (3) Commanding Officers from the Bulawayo Metropolitan Criminal Investigation Department. Structured interviews ensured participants had equal opportunities to provide information and assessed accurately and consistently. The researcher was able to evaluate competencies that are difficult to measure using other interviewing methods.

The researcher put a collection of pre-determined, standardised and identical questions from the interview schedule prepared by the researcher (Welman et al., 2005: 165) to the participants face-to-face and recorded their responses and at the same time maintained a social interaction. The researcher read the open-ended questions in same way and noted answers without comment. All responses were evaluated using the same rating scale and standards.

The researcher used semi-structured interviews for the three (3) purposively selected Police Public Prosecutors based at Tredgold Magistrate Court and Western Commonage Court respectively. This technique is used to collect qualitative data by setting up a situation that allows participants the time and scope to talk about their opinions on a particular subject. According to Oates (2012:192), semi-structured interviews provide a positive rapport between interviewer and interviewee and it is an efficient and practical way of getting data about things that can't be easily observed. It has high validity as interviewees are able to talk in detail and depth with little direction from interviewer. Complex questions and issues can be discussed and clarified. The problem of researcher predetermining what will or will not be discussed in the interview is resolved and it is easy to record interview even with a video or audio tapes.

The researcher used open-ended questions in the form of an interview guide and the focus was on gaining an understanding based on textual information obtained. The questioning route was flexible although a given set of questions were covered and ensured that participants were not restricted by standardised questions. The researcher was able to get the participants to expand upon their answers, give more details and add additional perspectives.

Permission

On the 12th day of September 2013, the researcher was granted permission by the Commissioner General of the Zimbabwe Republic Police to carry out a research within the organization and interview members of the Police Force in the Bulawayo Metropolitan.

The permission covered the interview of the three (3) Police Public Prosecutors as they were serving members of the Zimbabwe Republic Police.

Consent

The researcher obtained consent from the participants after explicitly and truthfully explaining to them of the nature of the research and expectations. The interview fashion was clearly outlined to them and how information gathered from them will be used. The participants were informed that they reserved a right to decline any interview or withdraw even during the interview session (Oates, 2012:57).

Participants

The participants were a representative of the group and formed sum of Sample "A" Investigating Officers and their commanding officers and sample "B" of Police Public Prosecutors.

Preparation

In preparing the interview the researcher analysed the research problem and the content of information required from the interviewees and the participants most likely to provide the information (Welman et al., 2005:167). Oates (2012:187) says it will be ideal to gather background information on interviewees and their context. The researcher tested the correctness and thoroughness of the questions to elicit the required information. At least one practice interview was done with a willing friend. This enlightened the insights of cultural endowment of the participants and required improvements to the questionnaire were obtained (Welman et al., 2005:167-168). The process also depicted the amount of time that would be required for the questions.

After preparation of the interview guide the researcher notified the participants and called for appointments with full details of the interview and the time and days required for the interview.

Scheduling

The researcher obtained an agreement for an interview; explained the purpose of the interview and likely duration and the venue. As a former Police Office, the researcher is familiar with the regalia appreciated by the participants and upholding of social convention. The interviewees were advised on how the information will be recorded. The interview was conducted in the participants' offices where there were no disturbances or interruptions.

Interview

Before the interview, the researcher oriented participants as to what the research questions were, in a simple and understandable language without leading the participants and allowed them to entirely provide answers. The researcher managed time without interrupting the participants in the flow of the process. The responses were recorded verbatim.

Post interview

The researcher captured field notes and transcribed them immediately after the interview. After the interview the researcher wrote a thank note to the participants.

1.9.3 Case Docket Analysis

Yin (2003b) as quoted by Oates (2012:142), asserts that a case study is an empirical inquiry that investigates a contemporary phenomenon within its real life context, especially when the boundaries between phenomenon and context are not clearly evident. The researcher conducted case docket analysis on computer-related crime dockets recorded from the 1st January, 2010 to 30th July, 2011 because these have been completed, closed, categorised and filed sequentially in numerical order at the three districts purposively selected in the population target, namely Bulawayo West, Bulawayo Central and Bulawayo Suburban. The researcher used random sampling under probability sampling technique to select 12 dockets from each of the three districts crime

registers to draw a target population of 36 case dockets. The sequential filing of dockets in numerical order in each district made it simple to put all the population of dockets in a hat to draw out the required number of dockets.

On the 15th of September, 2013 the researcher was granted permission to carryout research in the Zimbabwe Republic Police by the Commissioner General of Police and the permission included perusal of dockets.

During the case dockets study the researcher sought for answers to the following questions:

- Were the search procedures executed in an appropriate manner?
- If the search was done with a warrant, was the warrant valid to satisfy the set out procedures?
- Does the copy of the search warrant in the docket precisely describe and state the items to be searched for?
- Does the information on the docket specify the premises to be searched, and state the reason for the search?
- If the searching was done without a warrant did the investigators observe the exceptions?
- How were searches conducted?
- Was evidence obtained from the searches admissible?
- If not, why was such evidence inadmissible?
- Do investigators have adequate resources to conduct meaningful investigations?

This assessment was achieved through studying of statements, investigation diaries and documents describing exhibits.

1.10 DATA ANALYSIS

According to Oates (2012:38), data analysis is looking for relationship or themes and drawing up of a conceptual framework to analyse data and Welman et al. (2005:210) asserts that data analysis helps us to investigate variables as well as their effect, relationship and patterns of involvement within our world. Singh (2006:223) mentions that it involves breaking down existing complex factors into simpler parts and putting the parts together in new arrangements for the purpose of interpretation. The researcher started data analysis by reading through the data to identify the following key themes; according to Oates, 2012:268);

- Segments that were not needed for the study.
- Segments that described the research context.
- Segments that were relevant to the research question(s).
- The researcher started by analysing raw data collected using selected data-generation methods. The data was organised and then categorised according to the key theoretical concepts; “forensic investigation”, “criminal investigation”, “evidence”, “computer-related crime”, “computer forensics”, “search and seizure” and “search warrant”. The researcher used a filing system by opening a file for each key theoretical concept. Information under each category was then filed chronologically.
- Common themes were identified in order to establish a direct and systematic approach when analysing the data
- Information was compared within categories in order to identify variations and similar meanings. Data collected was screened daily and similar data as well as variations were categorised together and where there was a need for information it was easily identified, obtained and then categorised.
- A table was used to categorise the themes; computer related crime, search warrant, evidence, forensic investigation, search and seizure and to elucidate the unique nature of computer-related crime evidence and peculiarities of computer-related crime investigations and the pattern of investigations, search and seizure procedures adopted by investigations

1.11 METHODS TAKEN TO ENSURE VALIDITY

According to Welman et al. (2005: 142), validity is the extent to which the research findings accurately represent what is really happening in the situation; and Leedy and Ormrod (2010:29) say validity of a measurement instrument is the extent to which the instrument measures what it is intended to measure and that it measures it correctly.

To ensure validity, the researcher selected thirty three (33) samples, thus twenty seven (27) investigators, three (3) Commanding Officers and three (3) Police Public Prosecutors. These were logically homogeneous out of the population using appropriate purposive sampling methods and they were a representative of all investigators and Police Public Prosecutors involved in the investigation and prosecution of computer related crime.

The researcher used confidentiality and informed consent with the participants. The participants were afforded freedom to withdraw consent at any time during the interview session. A causative environment that is favourable to the participants was created and similar questions were read and explained without leading the participants. The interview questions were based on the identified research problem, research questions and biased to the participants' experiences, observations, back ground and feelings. The Police Public Prosecutors were asked somewhat different questions to the Investigators because of the variations on the level of data required from each entity. The benefit of the personal interview was that where there was ambiguity the researcher had an opportunity to clarify and explain issues.

The researcher used triangulation to ensure the validity of data. According to Oates (2012: 37), triangulation is the use of more than one data generation method to corroborate findings and enhance their validity. It is used to explore one set of research questions and cultivating informed approach from different dimensions. The researcher corroborated the interview data obtained from the research questions by consulting other sources of information such as dockets, literature research in text books, journals,

periodicals and internet to provide some back up for the validity of the methods used as asserted by Singh (2006:80). All sources were *cited* accordingly.

The researcher made use of approved and valid data analysis techniques tested by other researchers in order to attain appropriate and valid research results. Other researchers are likely to arrive at the same results if they use the same methods.

1.12 METHODS USED TO ENSURE RELIABILITY

According to Welman et al. (2005: 145), reliability is concerned with the findings of the research and relates to the credibility of the findings. Leedy and Ormrod (2010:29) mention reliability as the consistency with which a measuring instrument yields a certain result when the entity being measured has not changed. As a way of ensuring dependability and repeatability the researcher used reliable sampling techniques in coming up with participants and case dockets. No participants were foreign to collection of computer-related crime evidence. The researcher did not use unfamiliar terminology or technical terms. He was concise without being ambiguous and maintained neutrality and ensured all questions were appreciable to all participants as underpinned by Welman et al. (2005: 180).

The researcher ensured that the interview schedule yielded the same results if given repeatedly to the same participants. Dockets where persons were convicted, acquitted, withdrawn before plea, or where the Prosecutor declined to prosecute were analysed. The researcher employed non-probability sampling techniques, thus, purposive sampling to choose three stations in Bulawayo Metropolitan and cybercrime investigators. The researcher used literature that was readily available and could be collected unobtrusively and other researchers could easily check and scrutinize on them. This approach helped to give credibility and reliability of literature.

1.13 ETHICAL CONSIDERATIONS

According to Welman et al. (2005: 181), the principles underlying research ethics are universal and concern issues such as honesty and respect for the right of individuals. Guided by the foregoing authors, the researcher tried not to put pressure or create anxiety on participants, but ensured;

- That there is voluntary informed consent by obtaining permission from the Commissioner General of the Zimbabwe Republic Police on the 12th of September, 2013 to carry out a research in the Zimbabwe Republic Police. The participants were thoroughly and truthfully informed about nature of the research, their involvement, benefits expected from the research and the method of the interview. They were also informed that there will be no incentives and how the findings will be disseminated (Oates, 2012:57). The researcher apprised them of their rights not to participate and the right to withdraw from the research at any time.
- Right to anonymity; the participants were informed of their rights to protection in relation to their identity and location to avoid embarrassing repercussions on them (Welman et al., 2005:201).
- Right to confidentiality; participants were informed that the data obtained from them is kept confidential.
- Protection from harm; the participants were given assurance that they will be indemnified against any physical and emotional harm (Welman et al., 2005:201).
- The researcher guarded against manipulating participants and use of unethical tactics or techniques of interviewing.
- The researcher did not intrude unnecessarily into the participator's core activities.
- The researcher recorded data accurately and did not keep quiet about data that did not support the researcher's case or manipulated data. An element of honesty and openness was displayed without falsification or fabrication. (Oates, 2012: 61).
- The researcher followed appropriate professional codes of conduct as is required in the Zimbabwe Republic Police Criminal Investigation department.
- The researcher afforded full credit to the original authors, with enough information in the reference so that any subsequent reader can find the same material to avoid plagiarism.

1.14 RESEARCH STRUCTURE

Chapter one: General Orientation

Chapter two: Computer-related Crime: Discussion on the fundamental overview of computer-related crime as it relates to forensic Investigation.

Chapter three: Searching procedures during investigation of computer-related crime for evidence derived there from to be admissible in court. It addresses fundamental principles related to the correct procedure to be followed during search of evidence. It deals with legal concepts of search with or without a warrant and various search warrant exceptions. It discusses the admissibility of evidence extracted during searching and how the integrity of such evidence can be sustained.

Chapter four: Findings and Recommendations. Concludes the research with divers recommendations related to each finding and the summary of the *supra* chapters.

CHAPTER 2: COMPUTER-RELATED CRIME

2.1 INTRODUCTION

According to Chawki (2005:25), the chronicle of computer-related crime is commensurate with the history of computers. The subsequent computer-related crime studies with applied scientific research methods are traced back to the 1970s of which the majority of cases were neither recorded nor detected. Computer-related crime is globally perceived as arduous to comprehend or conceptualize. It is viewed as violation of prescribed legislative enactments using a computer or the use of computers to commit other crimes. According to Goodman (1997:468), there is no consensus at all levels in precisely formulating a definition of computer-related crime as the term itself encompasses an extensive range of violations that unanimity has been an elusive goal. The researcher noted that divers' jurisdictions have promulgated what they term computer-related crime and notably, all include the essential elements of computer as a target of crime, a tool of crime or incidental to the crime.

Mobbs (2003:1) postulates that computer-related crime is an often used term with a very vague meaning. The relevant legislative enactment on computer-related crime is trailing the actual practice of computer-based crime. In an attempt to define the computer-related crime, Mobbs (2003:1) looks at the computer as a tool used to peddle malicious damage or illegal activities. Mobbs (2003:1) narrates how technology in the form of internet and other related networks have aided computer-related crime to be carried beyond borders. He lists divers essential elements in which computers can be used to commit crimes such as fraud and forgery in which computer -related crime laws are generated to deal with, to damage or modify other computerized systems. He further posits that this also include activities that cannot be prosecuted but fall short of satisfying illegal essential elements. The technical principles hinder the possibilities to legislate such actions.

According to Farmer and Celentano (2000:1), whilst computers afforded some advantages to businesses, governments, schools and individuals there are inadequate

laws to combat the dark side of the computer revolution. Nominal resources enable people and institutions via computers to leap states and national boundaries to benefit from innumerable opportunities. They, however, often fall prey to predators with prosecution almost difficult to pursue.

This chapter deals with the concept “computer-related crime”, the term “computer forensics”, different types of crime scene, the rights that equip the investigator with a mandate to investigate crime, the qualities the investigator should possess in order to investigate computer-related crimes, the responsibilities of an investigator, the purpose of investigations, the different types of evidence, types of evidence found at the computer-related crime, where computer related crime resort under traditional crimes, ways a computer can be used in crimes, classifications of computer-related crime, approach to computer-related crime scene and investigation models developed by computing experts. There is need to define computer-related crime to mark its distinction from traditional crime.

2.2 THE MEANING OF COMPUTER-RELATED CRIME

According to Aslan (2006: 130), there is limited scholarly collaboration as to the definition of computer-related crime. Hollinger (2000:77) highlighted that authors have limited consensus on definitions. Forester and Morrison (1991:305), are of the opinion that the absence of such lucent definitions has stunted development of decisive and relevant compatible solutions to the computer-related crime. Parker (1989: 2) defines computer-related crime as- “Intentional or malicious acts associated with computers as instruments, subjects, objects or symbols in which a victim suffers a loss and a suspect makes a gain”. However, the essential elements gain and loss in the foregoing definition diminish actions perceived as criminal and this could be an oversight to reality. Some acts viewed as malicious in the former definition may not necessarily result in a competitive gain. Chawki (2005:9) and Parker (1989: 2) define computer-related crime as “any recorded incident linked with computer technology in which there is potential proprietary prejudice or loss or where there is actual loss to another person and intentional gain by another”. In

addition, Kunz and Wilson (2004:7) mention that the perpetrator should have computer knowledge in order to commit a computer-related crime.

Computer-related crime is an unlawful act that is perpetrated through use of a computer as a principal tool (Icove, Seger and Vonstroch, 1994:464). Whereas, Alexandrou (2011:1) defines computer-related crime as any violations of criminal law that involve knowledge of computer technology for their perpetration, investigations, or prosecution. Alexandrou (2011:1) underpins Masango (2004:70), who earlier on in his definition, added the following categories as the essential elements of computer related crime; [1] crimes in which computer hardware, peripherals and software are targets of the crime, [2] crimes in which the computer is the immediate "subject" or "victim" of a crime and [3] crimes in which computer serves as means by which ordinary crimes are committed.

In defining computer-related crime, the foregoing authors attempted to portray that for computer-related crime to be qualified a computer has to be used by a person with the knowledge of computer technology. The person must be in pursuit of something of value. Goodman (1997:468) and Branigan (2004:101), support this by stating that computer-related crime occurs when the criminal uses technology to commit crime or criminally attacks technology thereby making it target of the crime. Icove et al. (1994: 464), further explain that the computer is the target or tool of the crime. Furthermore, Tavani (2000:4), mentions that computer-related crime constitutes "unlawful and intentional acts committed from or against a computer or network." Sarrab, Aldabbas and Elbasir (2013) corroborated Tavani (2000:4) and defined computer-related crime as any distrustful practice achieved using computer and network to breach the promulgated legislation enactments. This explanation includes the use of digital resources to commit traditional crimes. Hinduja (2007:3), concurring with the Royal Canadian mounted police guideline (2010:1) defines computer-related crime as an illegal act fostered or facilitated by a computer, whether the computer is an object or instrument used. Mumbai Police Cybercrime Report (2004:3) explains in simple terms; that it is any crime where the computer is a target, is a tool of crime and is incidental to the crime.

Twelve participants in sample A, when asked what they understood of the concept "computer-related crime", stated that computer-related crime consisted of any traditional crime capable of being committed in an electronic environment. The three participants in sample B shared the same vision and went further to elaborate that the benefits accrued from some criminal acts should be both tangible and intangible. Marshall, Robinson and Kwak (2005:3), corroborated that computer-related crime is a set of crimes in which digital data or software play a major role of which the majority is intangible, thereby igniting unique legislative attention to computer-related crime. Chik (2011), reiterates that computer-related crime envelopes violations against the computer, software, data and the computer itself as a processing tool. Eleven participants in sample A suggested that for computer-related crime to sustain, the definition should include all possible acts that are used to violate a computer itself, computer system and its network. Seven participants in sample A said it is an unauthorised use of a computer to commit a crime. The participants were guided by the Zimbabwe Criminal Law (Codification and Reform) Act 23 of 2004 which in its definition of computer-related crime include, unauthorized access to or use of computer or computer network, deliberate introduction of viruses into a computer or network, unauthorized manipulation of proposed computer program and unauthorized use of a computer.

All the participants agreed that, the computer is used as a tool to commit crime and may not necessarily be the target. The researcher concurs with the foregoing, in that a mere theft of a computer does not constitute a computer-related crime. The storage of tainted information in a computer would not be classified as computer-related crime. The researcher's opinion is that the perpetual advancement in technological environment has enabled divers' crimes with new elements to emerge in the environment. This has made it challenging to qualify a unanimous definition of computer-related crime hence the locution "computer fraud, technological crimes and cyber related crimes." In another school of thought Magnin (2001:2) explains literally that a "computer-related crime" has two elements: "computer" and "crime". The two should be in relationship to complete the

essential elements of the crime although in some instances the relationship could be indirect where a third presumed innocent victim is manipulated by the perpetrator.

The researcher's views are that computer-related crime definition seems to be very diverse. It is also debatable, particularly in trying to match the general crime essential elements with what is perceived in attempting to prosecute computer-related crimes. There seems to be no global uniformity in laws governing computer-related crimes. It would appear essential elements are extracted from judicial precedencies. An attempt to match essential elements suggested in the foregoing definitions may be a conduit in the creation of an identical definition of computer-related crime. Kunz and Wilson (2004:7), acknowledge that invariant definitions of computer-related crime are extremely important in aiding investigators to understand their role and resources required to address computer-related crime. The definitional distinctions depict differences in addressing computer-related crime. Hinduja (2007:5), says the methods and procedures that address both computer-related crime and traditional crime are indistinguishable. This is because of repeated application ingrained in their adaptation of traditional crimes through technological growth**.**

2.3 COMPUTER FORENSICS

In the mid-1980s the proliferation of pragmatic problems associated with technological cases motivated computer technologist to devise software programs to solve these issues that were increasingly debilitating. In a bid to respond to such cases, investigation of computer-related crimes emerged as "computer forensics". According to Al-Fedaghi and Al-Babtain (2012:97), computer forensics is defined as "analytical and investigative techniques used for the identification, preservation, extraction, documentation, interpretation and analysis of computer media which is stored or encoded for evidentiary and root cause analysis." The foregoing definition portrays investigation as an aid to proceedings in a competent tribunal on matters associated to computers and networks. It also deals with acquisition and analysis of evidence presented in such a tribunal. Newsom (2006), suggests that computer forensics is the execution of computer probing and examination techniques with a bid to establish legal evidence. Information Security

and Forensics Society (2004:3), explains that computer forensics is a science of acquiring, preserving and documenting evidence from digital devices with storage capabilities for the purpose of presenting valuable evidence that is legally admissible. The foregoing definition suggests that handling of evidence in computer investigation must be done by a person knowing what type of evidence exists and where it can be found. In asserting this opinion, Patzakis (2003:6) added that the courts require appropriate collection and analysis of computer evidence in an investigation where a computer is a tool of the crime. Computer forensics is, therefore, the appropriate collection, preservation, analysis and presentation of such evidence as required by the courts. This should be done by a person with both computer scientific and technological expertise.

The three participants in sample B when asked of what they understood by the term "computer forensics", defined computer forensics as the use of scientific accepted methods to collect, preserve, validate, analyse, interpret, document and present digital evidence obtained from a computer for the intention of proving a computer-related crime. Fourteen participants in sample A defined computer forensics as the process of acquiring, analysing, examining and interpreting electronic content so that it is incontestable in court. Bui, Enyeart and Luong (2003:6) are agreeable to participants in sample A and highlighted that computer forensics involves the preservation, identification, documentation, extraction and interpretation of computer data.

Thirteen participants in sample A defined computer forensics as an application of computer investigation and analysis techniques in the interest of determining potential legal evidence. The participants defined in line with Bassett, Bass and O'Brien (2006:23), who state that computer forensics is the application of both computer investigation and analysis techniques to gather evidence for presentation in a competent tribunal. Therefore, computer forensics refers to the execution of well-defined structured investigation with well documented evidence to establish what transpired on a computer and identification of offenders. Three participants in sample A, mentioned that computer forensics is the close examination of computer technology as it logically links to the law.

Daley (2010:60), adds that computer forensics is standardized examination of data inherently domicile on digital media. This definition depicts the process of data retrieval and confines computer forensics to the *supra* process. Huebner, Bem and Bem (2007:16) express that the collection and analysis of data should be done in a concise manner without any distortion or bias in reconstructing previously recorded data. Data recovery is only one aspect of the forensics investigation (Bui, et al. 2003:6).

The researcher's opinion is guided by the *supra* authors and also having considered the prevailing essential elements. The entire computer forensics is the application of principles using tools and techniques to detect and process evidence for adjudication review in a court of law. According to Mundt (2009:05), there are typical phases in computer forensics which are system preservation, searching of evidence and reconstruction of event. Mundt (2009:05) further summaries that computer forensics ensures that evidence collected is not altered, any handling of evidence is documented and access to evidence is restricted to forensically competent persons. The foregoing fact is also presented by Patzakis (2003:06). A forensically competent person will ensure evidence is collected carefully and legally to eliminate possibilities of evidence suppression during trial (Bui et al., 2003:6).

Vidas (2006) in his definition seems to enroll all essential elements from most of the aforementioned authors and recapitulates that computer forensics traditionally includes preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of computer evidence stored in a computer. Computer forensics is a new phenomenon to competent tribunals. The current legislative enactments used to prosecute computer-related crimes and practices related to computer forensics are increasingly changing as most definitions are guided by legal precedents.

2.4 TYPES OF CRIME SCENES

Hana, Freitas, Oliveira and Bortolozzi (2008:419), define crime scene as a place where a crime occurs or is detected. This is so because the subsistence or non-actuality of some criminal act is proved by the evidence derived from a crime scene. Alifano (2006),

mentions the crime scene as the paramount site where investigations commence although there could be other additional and secondary scenes. The crime scene is susceptible to environmental changes leading to precipitate deterioration of evidence. Therefore, protection against contamination and annihilation is required before and during the processing of a crime scene.

Thirty participants in sample A, in describing the different types of crime scenes, mentioned types of crime scenes as either primary or secondary; the primary crime scene being where a crime actually occurred and secondary crime scene related to the crime but not the place of occurrence. Simlot and Christopher (2002: 6), support the views of the participants and point out that the primary scene is the location where the crime occurred and the secondary scene is all of the surrounding area outside the area but within the scope of the primary crime scene. Miller (2011:115), emphasizes that the diversity of crime scenes makes them unpredictable. Miller (2011:115), further stresses the *supra* opinion of Simlot and Christopher (2002: 6) and states two types of crime scenes, thus primary scene which is the environment in proximate of the occurrence within which evidence may be found. The secondary scene is an area, although not in the immediate proximity of the primary crime scene, may still afford evidence thereby connecting the suspects and victims to the crime. The foregoing statement suggests suspects and victims could be secondary scenes.

Douglas, Burgess, Burgess, and Ressler (2006: 28), argue that the primary sources of physical evidence are the victim, the suspect, and the crime scene and secondary sources include the home or work environment of a suspect. Alifano (2006), advances a diverse point and mentions that in divers' cases initial primary scenes may not always be the primary scene and there are times where actually secondary scenes create the fundamental principle or instauration of ensuing a criminal investigation and subsequent prosecution. According to Carrier and Spafford (2003:6), the primary and secondary crime scene concept is also applicable to computer crime scene. Carrier and Spafford (2003:6), further describe the computer crime scene as the virtual environment created by software

and hardware where digital evidence is located. The environment where the first criminal act occurred is the primary digital crime scene and succeeding scenes are called secondary digital crime scenes (Carrier and Spafford, 2003:7).

According to Carrier and Spafford (2003:10), to illustrate the digital primary and secondary crime scenes in a computer crime scene, the violated server would be the primary digital crime scene and the log server that was violated later to modify the logs relating to the intrusion would be a secondary digital crime scene. Baldwin (2011:4), explains the types of crime scene in a different manner as he says the primary area is where the principal objective of the crime was located and the secondary area are leads to the place of occurrence. Both areas should correlate. Lee and Pagliaro (2013:02), agree with *supra* authors on the primary and secondary scene and further assert that there are multiple ways to classify a crime scene. They summarise additional types of crime scenes as:

- The type of crime committed such as computer-related crime, fraud and etc.
- The physical location of the scene, thus whether it was indoors or outdoors.
- The physical condition.
- The boundaries of the scene, for example, bank, office or computer.
- The appearance of the crime scene, for example, whether it was organized or disorganized crime scene.
- The activity, thus whether the scene was active or passive.
- The size of the crime scene, for example, universal or microscopic scene

The researcher's opinion is that primary crime scenes in most cases are rich in substantial utilizable evidence than secondary crime scenes. It is, however, possible to commence investigations at a secondary crime scene and be led to the primary crime scene and subsequently to suspects or further evidence.

2.5 MANDATE TO INVESTIGATE CRIME

According to Alifano (2006), an investigator is a person with collaborative common sense, judgment, intellect, experience and nurtured instinctual qualities along with a comprehension of relative technical knowledge. This suggests that not every person can be mandated to investigate. Ask (2006:1) agrees that criminal investigation is compounded and psychologically absorbing. According to the Constitution of Zimbabwe Act No 1 of 2013, the police service shall be responsible for detecting, investigating and preventing crime. The interpretation of the foregoing legislation is that only Zimbabwe Republic Police has a mandate to investigate as this is reiterated in the Zimbabwe Republic Police Act 22 of 2001. According to the General Instructions Regarding Investigation & Enquiries (2013:1), a similar scenario prevails in India where only investigators of the Central Bureau Investigation (CBI) are mandated to investigate offences notified by the Central Government as depicted in section 3 of the Delhi Special Police Establishment Act of 1946.

Twenty six participants from sample A, in explaining the rights that mandate investigators to investigate crime, believed only the State police had the mandate to investigate and present the matter to a competent tribunal for prosecution. Whilst four participants in sample A agreed that State police had a mandate to investigate as enshrined in the constitution of Zimbabwe, they mentioned that the Zimbabwean laws provided for private investigators. This assertion is affirmed in section 10 of Chapter 27 in the Zimbabwe Private Investigators and Security Guards (Control) Act 8 of 1988 that mandates for the appointment of a Controller of Private Investigators and Security Guards. The private investigators are only limited to carrying out business at the request of any person as a client of the business and not as a member of the public for reward. The information private investigators provide should only be relating to personal actions, behaviour, character, financial position, the business, occupation, the identity, whereabouts of any other person, suspected criminal offences or civil wrongs, not being information which is contained in a public document.

In licensing the private investigators, the Commissioner General of the Zimbabwe Republic Police has to approve the application. This arrangement confirms the State police as the only entity that has a mandate to investigate all criminal cases both in private and public environments. Other Financial institutions and some of the banks have internal structures termed Group Forensic Services (GFS) with a mandate to investigate allegations of criminal, civil and other acts that pose potential risk and other crimes perpetrated against the financial institution. The investigative body has its investigative mandate from the most senior executive granted through a policy signed by top management within the organization. They have the power to investigate an incident by interviewing any employee of the organization, without regard for seniority or influential position (Stephenson, 2000:217). Prosecution is in the public interest and therefore can only be done through the State police. According to Audit and Investigation Guidelines (2012:4), the latter investigation mandate is similar to the mandate that empowers the office of audit and investigators. They derive their mandate from the United Nations Development Programme (UNDP) to investigate all allegations of fraud and corruption against UNDP, committed either by UNDP staff members, other parties or entities, deemed to be detrimental to UNDP.

The opinion of the researcher is that the investigation mandate outlines the right of the investigators in relation to interviewing parties and collection of evidence for such purposes. The methods, code of conduct and ethics in relation to the investigation are established prior to the investigation.

2.6 QUALITIES OF COMPUTER-RELATED CRIME INVESTIGATOR

According to Williams (2011:29), the accessibility and use of technology, the heightening of virtual storage, advancement of and the merging of mobile and traditional computer technology has ensued in investigations having a digital element of some description. Investigators should have a comprehensive appreciation use of digital evidence to effectively achieve interviews of witnesses and suspects. Investigators are expected to cultivate proper strategies to identify the existence of digital evidence, secure and interpret that evidence. Williams (2011:32), illustrates that investigators should be

acquainted to capture, search and data seizure at the crime scene as well as examine and interpret the collected data and interview witnesses and suspects.

The Quality Standards for Investigations (2011:2) state that “Individuals assigned to conduct the investigative activities must collectively possess professional proficiency for the tasks required.” In view of the foregoing opinion, Kunz and Wilson (2004:4), in their discussion point out that investigator must be trained in computer science or computer forensics to properly investigate computer-related crimes. Kunz and Wilson (2004:4) agree with Collier and Spaul (1992:314) that a computer-related crime investigator should be able to merge into a multi-disciplinary team equipped with the investigative skills to interview suspects and witnesses and legal skills with an insight of computer-related crime legislative enactments and the laws governing relevant evidence. Kunz and Wilson (2004:4) and Collier and Spaul (1992:314), further assert that the computer-related crime investigator should also possess court room presentation skills in testifying as a witness; and computer skills with capabilities to reveal methods on how the crime was committed and reconstruct the scene, collect computer evidence and canvass proceeds of the crime.

Sogbaike, David, Esther, and Victor (2014:36), concur with some relevant investigator skills outlined by Collier and Spaul (1992:314) that the investigator should be able to gather incident traces from a computer-related crime into acceptable legal evidence in a form that tells the complete and convincing story without misrepresenting or altering any of it. Participants were asked of qualities that investigators should have in order to investigate computer related crimes and eleven participants from sample, A mentioned that the investigator should be able to acquire and preserve computer evidence, do documentation and analysis of collected data. This view is shared with Home Office Cyber Crime Strategy (2010:26), which stresses the investigator should have the aptness to trace offenders and victims through recovery and analysis of computer-related crime evidence.

Seven participants’ from sample A, stated that investigator should be able to recover evidence including deleted files. Bui, et al. (2003:32) further explain this position and

suggest an investigator should have appreciation of fundamental technologies related to appropriate gathering of information and ensuring its validity as evidence in court. The qualities extend to abilities in acquiring, authenticating and analyzing data stored in electronic devices on all operating systems. Bui et al. (2003:32) further mention that a competent investigator should comprehend the detection and tracing of divers' computer users including deleted files using technology at hand.

Twelve participants from sample A indicated that the investigator should be able to collect evidence from a computer-related crime scene, do meaningful analysis and investigations. Goodman (1997:492), in a wide discussion of building a computer competent investigator emphasizes that computer literacy should be a mandate to enable the investigators to ask relevant questions in their investigations quest. Goodman (1997:493) is, however, quick to mention that the investigator must be aware of procedures to determine when a computer-related crime expert should be invoked as some evidence collection might require highly specialized technical work. Ryder (2002:6) states that the inherent and distinguished characteristics of a computer-related crime investigator should have computer systems experience in programming, normally used operating systems and applications including appreciation of decipherment and decryption. Ryder (2002:6) further emphasizes that the investigator should also possess; strong analytical skills, endure to invest time in taking computers apart in search of evidence, strong computer science fundamentals, comprehend security vulnerabilities, intense system administrative abilities, robust verbal and written communication capabilities, appreciate current intruder tools and be familiar with the newest forensic tools. Collier and Spaul (1992:314) add that the investigator should have intense comprehension of the rules of evidence and evidence handling and proficiency to be an expert witness in a court of law as described by Collier and Spaul (1992:314).

Furthermore, Ryder (2002:6), explains that a computer-related crime investigator should be equipped with basic knowledge of primal methods and techniques. In a diverse opinion Pena (2000:18) further outlines that the characteristics that complement the qualities of

a computer-related crime investigator should include the ability to gather information but verify its truthfulness and credibility and eager to investigate and learn the facts and truth about people, places and how they related to objects. The investigator should develop the ability to take accurate notice of evidence possess and unbiased and unprejudiced mind (Pena, 2000:18). It is the researcher's opinion that establishing a rapport with victims and witnesses is one of the prime facilitators of an investigation by being patient, courteous, and sympathetic during an investigation. Becker and Dutelle (2013:19) agree with both Ryder (2002:6) and Pena (2000:18) on the qualities of an investigator that he should be equipped with computer skills and competencies and amongst other things bear the qualities in deductive and inductive reasoning, analytical and critical thinking, ethics and integrity, language and communication. The aforementioned scholars further agree that the investigator should also be aware of constitutional law, law of evidence and its admissibility and evidence related computer forensics.

According to the researcher's opinion as guided by the foregoing sources, the computer-related crime investigator should possess the desideratum appreciation, techniques, competencies, philosophies, cognition and understand fully potential criminal exploitation of computer technology. She/he should be able to apply such supplementary technical knowledge to the type of computer-related crime investigation being conducted. The investigator should be familiar with the use of computer systems both software and hardware as an aid to investigative process. She/he should be familiar with proper means of obtaining, preserving and analysing evidence and other pertinent data. The investigator should also be able to deliver oral and written reports for presenting before the courts.

2.7 RESPONSIBILITIES OF AN INVESTIGATOR

According to Braga, Flynn, Kelling and Cole (2011:29), as from the 1930s to the 1970s criminal investigators have been engaged in reforming investigators' traditional thinking practice. This somewhat changed functionalities and the role of criminal investigators. Braga et al. (2011:30) identify investigators in the United States, Australia and United Kingdom as leaders in recognizing that the responsibilities of criminal investigators need expansion from a sole focus on traditional investigative activities to broader strategies

where technology plays a major role. According to Becker and Dutelle (2013:19), the responsibility of the investigator has been intensified on account of the evidence collected that has increased in value in the hands of forensic specialists. Becker and Dutelle (2013:19) illustrate that forensic specialists know how to retrieve the evidence but rely on the investigator to put its meaning into context. This is because investigator's responsibilities are to seek for evidence and weigh its significance.

The investigator therefore needs only to identify prospective evidence and leave it to the trained personnel to process it. Braga et al (2011:3), listed the responsibilities of investigators as follows:

- Interviewing victims, witnesses and offenders
- Cultivating and managing of informants.
- Administering disguised surveillance using prime surveillance technologies.
- Establishing witnesses and intelligence source.
- Preserving and developing evidence.
- Compiling criminal dockets for prosecution and seeking guidance from prosecutors during the preparation and during the trial.
- Executing witness preparation for the trial.
- Arranging a sequence of investigative steps for a successful investigation.

Six participants from sample A, when asked what the responsibilities of an investigator were during the investigation of crime, said criminal investigators' responsibility is delivering justice to crime victims and seven participants from sample A, posited that during the investigation of crime, investigators are responsible for ensuring preservation of property and life. The views by the above participants are in line with what Alifano (2006) says that the responsibility of the criminal investigator reaches far beyond that of mere definitions. Crime detection and investigation are major responsibilities and when these are undertaken appropriately other responsibilities such as the protection of property, preservation of life coupled with maintenance of peace are realized.

Eight participants from sample A, described the responsibility of an investigator as to arrest and subsequent conviction of a criminal offender. Ask (2006: 3), is agreeable when

he points out that the responsibilities of the investigator is to compound clues from diverse sources, arrive at a logical account of the critical event and to acquire information that can be used as evidence in court. Nine participants from sample A, said investigator's responsibilities are more inclined effectively, efficiently, and resolutely to the crime problem in general. According to Harvey (2011), the criminal investigators responsibility is viewed as a central role in crime fighting and solving crimes. In the same context, Tibasana (2001:164) noted the responsibilities as to prevent the commission of offences, to apprehend offenders and would be offenders. This responsibility is influenced by the prevalence or extent of the crime. The foregoing suggests investigator's responsibility is both a reactive process responding to individual crimes and intelligence driven proactive work in targeting suspected individuals or crime. This process is charged with appropriate appreciation of crime, its essential elements and how relevant evidence can be collected by the investigator at the crime scene during investigations.

The researcher as guided by Braga et al. (2011:3), is of the opinion that the investigator's responsibility is to uncover leads through evidence search, collection, and witness's interviews, analyze findings including technology-related crimes such as computer crime and testify in court. The responsibility starts with the scrutinizing of evidence at the scene, collaboration with others to share information, coordination of activities and the findings of his examination. The investigator decides what evidence is relevant to the case and the testimony expected in court.

2.8 OBJECTIVE OF INVESTIGATION

Investigation is defined by the Philippine National Police Criminal Investigation Manual (2011:1) as the gathering of details to identify and locate the suspect in order to provide evidence of his guilt. Law Reform Commission Act (2005.1) sharing the same views with Rossmo (2005:18) and Philippine National Police Criminal Investigation Manual (2011:1) suggest the objective of investigating a criminal offence is to gather evidence, identify perpetrators of the crime and present evidence before a court so that guilt or innocence may be decided. Philippine National Police Criminal Investigation Manual (2011:1) further states the investigator seeks to determine six fundamental points of investigation, listed

as; the type of crime committed, the modus operandi, who committed the crime, the place of occurrence, when did it occur and why it occurred. Alifano (2006:2) sharing the same opinion stresses that the objective of investigation is to find answers to the questions; when, where, who, what, how and why. According to Becker and Dutelle (2013:17), the objectives of investigation are to uncover crime, identify, profile and determine suspects, establish, note and process evidence whilst observing all legal admissibility concepts, apprehend the perpetrators whilst observing the statutory concepts provided by and in accordance with the constitution, recover property in conformity to appropriate searching and seizure procedures, prepare for trial including completing accurate documentation and secure conviction of the accused through testimony and present legally obtained evidence and statements.

Rossmo (2005:2), in conformity with the *supra* discussion maintains the objective of investigations is to locate the criminal, thus suspect identification and to prove the accused's guilt through case building. Each of the foregoing objectives require different mental processes and actions. This can be achieved by means of physical evidence, witnesses or confession. Brown and Heinemann (2001:3), mention that the objective of criminal investigation is to establish the magnitude possible and the actuality of events that constituted to the commission or omission of the crime. Brown and Heinemann (2001:3), Becker and Dutelle (2013:17) and Rossmo (2005:2), posit the objective of investigation is to establish if a crime has been committed, arrest suspects within the confines of law, recover stolen property using all legal possible means, use legal means in obtaining information and evidence to identify the person responsible for committing the crime and to present appropriately and accurately compiled documents to the prosecutor.

Thirty-six dockets analysed had victims reporting their cases and investigators responded to gather evidence. Brown and Heinemann (2001:3), further indicate these objectives can only be attained by an investigator who gathers all facts that tend to prove or disprove a person's involvement in a criminal act or omission, the truth then submitted for judicial

examination. The investigator should also be mindful that not all crimes are solvable. Sixteen participants from sample A claimed the objective of investigation is to gather evidence for prosecution and the foregoing assertion is listed as one of the objectives by both Becker and Dutelle (2013:17) and Rossmo (2005:2). Fourteen participants from sample A concluded the objective of investigation is to locate suspects and prove a case against them. This is a general summary of discussions portrayed by Brown and Heinemann (2001:3). Rossmo (2005:18) reiterates that criminal Investigation process should seek the truth, without fear or favour. It should be conducted in an unbiased manner and professionalism must be demonstrated.

The researcher is of the opinion that the objective of the criminal investigation is to establish that a criminal act was committed and then identify and apprehend the offenders using modern technology and forensic sciences. The objective stretches to the recovery of property and retrieval and maintenance of evidence. The investigations that meet the objectives are critical to the prosecution of offenders.

2.9 PURPOSE OF INVESTIGATION

According to Alifano (2006:2), criminal investigations are conducted primarily for the prevention of crimes and detection of crime. Moore, Trojanowicz, and Kelling (1988: 2) emphasize criminal investigations do have preventive effects at least as an inferred general concept. The successful prosecution of offenders' acts as deterrence to would-be offenders and any successfully prosecuted investigation incapacitates criminals with a capacity to commit further crimes. Fourteen participants from sample A stated that the purpose of investigation is to establish a solution to managing crime by detecting crime, arresting and punishing offenders. Homel (1994:6) and Moore et al. (1988:2) support the view that severe punishment and custodial sentencing serves as a general deterrence. Custodial sentence incapacitates offenders for a considerable time preventing them from committing further offences. There is also an element of rehabilitation whilst serving a custodial sentence or engagement in other programmes that may divert the offender from criminal tendencies.

Six participants from sample A, stated that the purpose of investigations is a responsive method of solving crime; and the Guide for Virginia Law Enforcement (1997:1) added that there is a growing emphasis on the purpose of reactive investigation, arrest, and punishment as way of preventing crime and substitution of preventive tradition. Ten participants from sample A noted the purpose of investigation as a reactive action to reduce and manage crime. Braga (2008:7) and Karn (2013:36) confirm that investigation is a component of professional crime reduction. They stress that, however, the prevention concept rests on the successful investigations by reputable investigators with crime solving abilities. The researcher's experience is that the purpose of investigation is achieved when there is apprehension and prosecution of offenders. This process will see offenders removed from the environment and circumstances where they are prone to commit crimes. They are afforded rehabilitative environment and this also eliminates recidivism.

2.10 THE DIFFERENT TYPES OF EVIDENCE

According to Masango (1998:41), evidence is "all legal means, exclusive of mere argument which tend to prove or disprove any matter of fact, the truth of which is submitted for judicial investigation". Sommer (2013:31), defines evidence as that which is presented before a court to persuade it to reach a particular view of events which must be in dispute. Nemeth (2011:1), mentions that in the absence of evidence, there is no proof; without proof, burdens are not met and convictions, verdicts, or judgments will be insurmountable. Evidence directs the courts and the practitioners arguing for its cause toward actions to be taken. Nemeth (2011:2), further argues that evidence is not always a mirror image of reality. Its representation may be influenced, slanted or distorted by the person inspecting it. According to the United Nations Office on Drugs and Crime Manual (2013:26), evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. United Nations Office on Drugs and Crime Manual (2013:26) further explains electronic evidence as all such material that exists in electronic or digital form that can be stored or transient. The evidence exists in the form of computer files, transmissions, logs, and metadata or network data. Sommer (2013:32), summarizes

that computer crime evidence must have all the attributes of other types of admissible evidence and lists the following six types of evidence;

- Real evidence- where there is an object or exhibit which can be produced before the court and examined in court.
- Documentary evidence- is a business or other record in any form whose authenticity has been proved and is examined for its contents in court.
- Testimonial evidence- where the memory testing is done by the court on a witness who perceived the crime being committed with his own eyes.
- Technical evidence- is where a forensic technician after some procedures on original “real” evidence produces some results. Technical evidence is not expert evidence as it does not give opinions.
- Derived evidence- is a chart or video created from primary evidence to demonstrate how certain conclusions might be drawn.
- Expert evidence- consists of opinions of an expert in a particular field after carrying out a specified inquiry.

Participants were asked to describe different types of evidence and three participants on sample B named the types of evidence as best or secondary, direct or circumstantial or indirect, oral or documentary, hearsay or original, conclusive and *prima facie* evidence. Masango (1998:42), affirms this by stating that there are six types of evidence although in his discussion he proves that types of evidence are interrelated to Sommer (2013:32) assertions. The discussions, however, exclude technical and derived evidence and he seems biased to traditional crime evidence. Masango (1998:42) lists the six types of evidence as;

- Evidence may be best evidence or secondary evidence- that is, evidence which per se indicates that there is no better evidence available regarding the question in issue and is regarded by the law as the most reliable evidence. The term “best evidence” is principally used in relation to documents. The document itself being the best evidence of its contents. Secondary evidence is evidence that per se

indicate that better evidence is available on the point in question. Secondary evidence is not admissible if best evidence is available.

- Evidence may be direct, circumstantial or indirect- direct evidence is either evidence given by a witness who actually perceived a fact in issue or evidence of a fact actually in issue. Circumstantial evidence is not of a fact directly in issue but a fact relevant to the issue and indirect evidence is evidence other than direct and comprises circumstantial and hearsay evidence.
- Evidence may be oral or documentary- oral evidence is verbal evidence of a witness and documentary evidence is given by means of a document.
- Evidence may be hearsay or original- hearsay is testimony by a witness who did not actually perceive the fact in issue in his own senses but to whom another person imparted the fact. Hearsay is not as general rule regarded as evidence and correctly speaking it is wrong to refer to hearsay evidence. Original evidence is given by a witness who did actually perceive the fact in issue with his own senses.
- Evidence may be conclusive- this is evidence which must be accepted by the courts as conclusive proof of a particular fact. The only other kind of conclusive evidence arises from irrebuttable presumptions.
- Evidence may be *prima facie* evidence- It is distinct from conclusive evidence which in the absence of contradictory evidence is sufficient to prove a particular fact. It differs from conclusive evidence in that it can be disproved whereas conclusive evidence cannot.

Eleven participants from sample A listed the types of evidence as; direct, physical, trace, testimonial and circumstantial. Thirteen participants from sample A identified the different types of evidence as demonstrative, documentary, tracing, identifying, associative, corpus delicti, testimonial, physical and oral evidence. Six participants from sample A pointed out only two types of evidence, thus physical and documentary. Nemeth (2011:37-420), in his discussions on types of evidence agrees with Masango (1998:42), Sommer (2013:32) and participants on the types of evidence. He further focuses on

personal knowledge, opinion evidence and character evidence. Nemeth (2011:37-420) has listed the following seven types of evidence in his assertion:

- Direct Evidence- is evidence that proves a fact or concept directly other than by means of secondary illation or inference. It includes eye-witness testimony or oral confession of an offender.
- Circumstantial Evidence- refers to indirect evidence, for example a bullet in a murder case is only circumstantial evidence because it does not signify direct agency, although its peripheral power of proof shows an agency connection. Inferences are drawn from circumstances beyond the key action or parties.
- Testimonial Evidence- this is evidence solicited or provided under oral or written testimony, whether by oath or affirmation, whether at trial or in the discovery processes.
- Personal Knowledge- addresses the quality and integrity of testimonial evidence in whether the witness, either lay or expert, has some personal knowledge relevant to the case. A witness may not testify to a matter unless evidence introduced is sufficient to support a finding that the witness has personal knowledge of the issue. Therefore, evidence to prove personal knowledge may but need not consist of the witness' own testimony.
- Opinion Evidence- is only permissible when a lay witness possesses personal knowledge of the events and conditions that are the subject matter of testimony within his intellectual domain and not opinion about things. Opinion is limited to experts except; (a) rationally based on the perception of the witness and (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue. Expert opinion dwells much on both scientific and technical issues, and other specialized knowledge that aids the court understand the evidence or to determine a fact in issue. The opinions of experts are not permissible unless they are based on facts or data perceived by that expert or made known to that expert before the hearing and will be accepted if scientific evidence is not sufficiently reliable.

- Character Evidence- is central to questions of integrity and credibility. A witness whose reputation is in doubt will be less persuasive than the witness with a sterling reputation in the community. Character in this sense has both individual and communal qualities.
- Documentary Evidence- is the best evidence consisting of memorialized writings or other inscriptions such as confessions, pleadings, contracts, memoranda, checks, or fraudulent banknotes.
- Hearsay Evidence- is when statement is being testified to by a second or third party.

In comparing the types of evidence, the researcher noted that there is a difference between evidence in a computer-related crime and traditional forms of evidence. This is because computer-related evidence is intangible and mostly it is an electronic pulse or magnetic charge. The researcher acknowledges the foregoing sources that the types of evidence that relate to computer crime investigations were direct, real, documentary, and demonstrative. Much of the evidence submitted in a computer crime case is documentary evidence.

2.11 TYPES OF EVIDENCE FOUND DURING INVESTIGATION OF COMPUTER-RELATED CRIME

According to the United Nations Drugs and Crime Manual (2005:1), most of the evidence in computer related crime is intangible and ephemeral and this makes it difficult to investigate. Williams (2011:6) claims computer-based electronic evidence is subject to the same rules and laws that apply to documentary evidence. However, Kerr (2005:279) argues that the current laws are tailored only for the gathering of physical evidence and eyewitnesses' testimony and any application of that law to digital evidence retrieval produces misleading results. Whitley and Figarelli (2009:1), define digital evidence as information and data of value to an investigation that is stored in an electronic device, received or transmitted by an electronic device. It is located on the computer's hard drive and peripheral gadgets that include removable media such as thumb drives and Compact Disk-Read-Only Memory (CD-ROM) discs.

Sommer (2013:26) agrees with the United Nations Drugs and Crime Manual (2005:1) that digital evidence is not direct, readable or tangible. Sommer (2013:26) further explains that derived exhibits are susceptible to manipulation and presented away from the original point. This suggests that computer evidence is not only a record or document produced by a computer. Sommer (2013:26), adds that the challenge in computer evidence is that there could be an existence of a large number of original computer data. For example, computer hard-disk seized may contain a large number of directories of various files while what is produced in court may be a number of purportedly accurate printouts or screen dumps. The prospects of imprecise presentations are likely. Six participants from sample A stated that the types of evidence found at the computer-related crime consist of computer hardware, software, and data contained therein or taken from a computer. Eleven participants from sample A listed hardware and contents in the computer known as electronic evidence. Thirteen participants from sample A mentioned computer and its accessories and digital evidence. Three participants from sample B said the types of evidence found at the computer-related crime were; digital evidence such as content that is illegally possessed computer log files and the computer itself. All the types of evidence listed by the participants, one way or the other, form part of evidence found at the computer related crime. According to Chawki (2004:5), computer crime evidences are classified into three *infra* main categories;

- Digital evidence where information is transmitted or stored in electronic or magnetic form.
- Physical information where digital information is transmitted or stored through physical media.
- Data objects where information are linked to physical items.

Maghaireh (2009:137), explains that digital evidence is in three perspectives. The initial is computer generated evidence consisting of log files, cookies, metadata, Internet Protocol (IP) addresses and in divers' formats, data and programs that include e-mails, websites and chatting programs. This evidence can be presented before a competent tribunal using multimedia devices. The second is computer stored evidence that can be printed as hard copies or visually displayed on computer screen. In some instances this

evidence can be generated or hybrid. Kerr (2005: 282), says human beings interfere with computer programmes to create digital evidence but stored evidence is generated without human interference. The third perspective is a combination of both computer generated evidence and computer stored evidence. In this third category evidence is a mixture of both computer generated evidence which is virtually visible but is not printable. It is in the form of history of the web, log files, websites visits and metadata and computer stored evidence which is visible and printable in the form of e-mails, word files, spreadsheets and digital pictures. Maghaireh (2009:137) agrees with Ghosh (2004:27) and Kerr (2005: 282) that computer crime evidence is divided into three categories: records that are computer-stored, computer generated and records partially computer-generated and partially computer stored.

The difference is determined by whether a person or a computer created the substantive contents of the records. Computer stored records refer to documents written by a person in electronic form such as e-mail messages, word processing files and social network chatting. On the other hand, computer-generated records contain the output of computer programs without human intervention such as log files, telephone records and Automated Transaction Machine (ATM) transaction receipts. Ghosh (2004:27), further explains that records that are both computer-stored and computer-generated such as financial spreadsheet contain both human statements, for example, input to the spreadsheet program and computer processing in mathematical calculation performed by the spreadsheet program.

Chawki (2004:6), adds that computer crime physical evidence consists peripherals such as Central Processing Unit (CPU), including devices that allow for input and output of information. These peripherals which form the integral part of computer system are attached by cables to the CPU. The examples are monitors, key boards, mouse and printers. Chawki (2004:7), mentions that information consists of software such as magnetic disks or Compact Disk-Read-Only Memory (CD-ROMS) and data in the computer system. Chawki (2004:8), further breaks software into two categories, thus

system software managing the operation of the computer and application software that performs high level tasks. They all form part of evidence at the computer-related crime scene.

According to Welch (1997:56), the type of evidence found at a computer-related crime is physical evidence and computer-generated evidence. Welch (1997:57), further explains that physical evidence consists of the computer itself, peripherals, notepads, or documentation and lists four types of computer generated evidence as:

- Visual output on the monitor.
- Printed evidence on a printer
- Printed evidence on a plotter.
- Film recorder which may consist of magnetic representation on disk and optical representation on Compact Disk (CD).

Legally computer-generated evidence is deemed to be hearsay. This is because magnetic charge of the disk or the electronic bit value in memory, which represents the data, is the actual original evidence. The computer-generated evidence is viewed as a representation of the original evidence.

According to Al-Azhar (2010:1), the evidence found in a computer-related crime that requires digital forensic analysis is grouped as computer-based electronic evidence. Al-Azhar (2010:1), further argues that it is physical evidence as it is visually seen and is sought at the crime scene. The findings in the form of data or information stored in the evidence are called digital evidence. Below is physical evidence which might be found during the investigation of computer-related crime scene:

- Personal Computers
- Notebooks / Netbooks / Laptops.
- Mobile phones / Personal Digital Assistant (PDAs)
- Printers.
- Optical Media: CDs / Digital Versatile Disks (DVDs)
- Zip drives / Backup Tapes.

- Flash disks, Hard disks, Floppy disks.
- Modems / Switches / HUBs / Routers.
- Digital Cameras.
- Memory Cards.
- Dongles.
- Wireless Network Cards

Sommer (2013:26), listed *infra* as digital evidence which might be found in the contents of the physical evidence above and can consist of:

- Meta-data within files, that is not viewable with audit trail of the file creator, the times it has been edited and when it was lastly printed. Microsoft word processing and spreadsheet documents that contain extensive meta-data.
- Configuration data files and directory data which help a computer and/or application programs to behave in a particular way and which provide evidence of how and when the computer was used. This includes material found in the registry on a Windows Personal Computer (PC).
- Content consisting of the words and figures in a document including images, designs within an application file, web pages, database or selection, files downloaded and emails.
- Directory data containing details of name, divers associated date and time stamps and size.
- logging data files created by and operating systems application programs which either record activity explicitly as in audit trails and online keystroke captures, or which can be used to attempt to reconstruct events in the form of history, session, event and recent files.
- Material from back-ups in the form of data captured by the operating system as part of system recovery functions such Microsoft Restore Points.
- Forensically recovered data obtained from storage media which would not normally be seen in the form of undeleted files, files from slack space, swap files, caches, plus fragments of any of the above.

- Intercepted data from material obtained by placing a monitor across a network connection or telephone. This in turn divides into three: thus (1) traffic data on who called whom, when and for how long, (2) content as to what was said (3) subscriber data bearing information about who “owns” the line or connection.
- Expert interpretations which are based on any of the above in any combination.

The researcher agrees with the above *cited* writers that evidence found during the investigation of computer related crime include physical evidence, such as the computer itself, peripherals, notepads, or documentation, in addition to computer-generated evidence which is a representation of the original evidence.

2.12 THE DIFFERENCE BETWEEN COMPUTER EVIDENCE AND DOCUMENT EVIDENCE

According to the Law reform paper (2009:162), computer evidence incorporates data generated or stored in digital form following the use of a computer. It includes data entered manually into an electronic device. Computer evidence also encompasses computational transactions, automaton or information processed within the computer matrix. In view of the foregoing, Law reform paper (2009:162), further defined computer documentary evidence as whatever information entered, originated or kept in databases, operational systems, and applications programs. This also encompasses computer-generated models in which outcomes are inferred, electronic and voice mail messages held lethargically within a computer memory bank. Kurzban (1995:438), has an opinion in the foregoing discussion that there is no difference between computer-generated evidence and documentary evidence. Williams (2011: 6), illustrates that digital evidence is governed by the same rules and laws that apply to documentary evidence. Prosecution has to prove that the evidence produced is same as it was first taken into the possession of investigator. In court a document or a statement contained in the document produced by a computer is admissible as evidence as long as it was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.

The researcher did not pose this question to sample A as it is more relevant to tendering of evidence in court. Three participants in sample B, when asked of the difference between computer evidence and document evidence concluded that there is no difference in the law of evidence between computer evidence and documentary evidence. Sheppard and Duranti (2010), are of the opinion that electronic material tendered at a court should be treated as documentary evidence. This is because records offered as evidence at trial are subject to traditional admissibility rules consisting of authentication rule, best evidence rule, and the hearsay rule and its exceptions. Digital records are also governed by the documentary evidence provisions. Gray (2008:120), agreeing with Kurzban (1995:438) and Williams (2011: 6) explains that this is because documentary evidence is related and assumed to be paper but now it is defined as any type of recorded information. The evidence could be lodged in a computer, video or audio as it does not stand alone. Gray (2008:120) pointed out that issues produced, recorded, stored, processed, retrieved by a computer are documents and considered as primary evidence. Arunda (2014) conforms to the foregoing claim by Gray (2008:120) and notes that the definition of a document includes electronic records.

Sheppard and Duranti (2010), in their discussion share the same opinion with Kurzban (1995:438) and Williams (2011: 6) that documentary evidence adheres to best evidence rule in that it must be original. However, digital substances present a challenge to traditional rule. Therefore, this suggests that the concept of original is inconsequential in the digital area, although records have the force of originals. Wang (2008:47) describes data message as a form of writing in law and makes electronic evidence documentary evidence. Wang (2008:47), further argues that, on the other hand, electronic is a new form of evidence and different from documentary evidence because traditional documentary can be demonstrated on a visible carrier whilst electronic evidence is readable through electronic devices and software.

Makulilo (2006:59) points out that the term document has been defined in reference to tangible media whereas the computer has made it possible for a document to exist in intangible medium. For example, the soft copy falls outside the traditional definitions of document in most evidence statutes. Makulilo (2006:60), further discusses that the issue of original and copy between computer data and computer printout have unclear illustrations and the best evidence rule which requires production of original document in court has been infringed by digital technology. This also affects hearsay rule in its application in relation to the distinction between computer output from a human intervention and those automatically generated by the computer. Makulilo (2006:60) states that the authentication may also be affected particularly when it comes to foundation evidence related to the computer operation. According to the Law reform paper (2009:163), evidence required to authenticate a document is determined by the nature of the document in issue whereas traditional paper documents are authenticated by the testimony of the author or a person who witnessed the author sign the document. However, this is not applicable to electronic evidence.

2.13 RESORT OF COMPUTER-RELATED CRIME UNDER TRADITIONAL CRIMES

Alkaabi (2010:16) in his discussion says computer-related crimes fit within traditional criminal law categories as computers can be used to commit traditional crimes such as terrorism, copyright infringement fraud, theft, espionage or pornography. Kunz and Wilson (2004:11) earlier on argued that more often existing criminal categories are influenced to adapt new terminology to depict the essential elements of the computer-related crime. Traditional crime only takes a new dimension when a computer is used to commit it.

Traditional crimes in the form of murder, rape, burglary and arson, and among others involve, the use of excessive force could be an element, resulting in victims incurring injury whereas in computer-related crime, violence is not be an element, spoofing and phishing may be used to access personal information such as credit card numbers and steal from victims.

Both participants from samples A and B on being asked where computer related crime resort under traditional crimes could not provide answers. This was an indication that the

knowledge base was somewhat limited, or they were reluctant to provide the answer and, or felt they would contribute nothing in intellectual content. This was despite the researcher rephrasing the question and providing them with more time to think about it.

Davis (2010:16), notes that computer-related crimes are defined similarly to traditional types of crimes such as rape, assault, theft and robbery only that they are committed by the use of a computer or other electronic devises. Davis (2010:17) and Kunz and Wilson (2004:16) further explain that computer-related crime is merely a part of traditional crime and the difference is on the investigation and prosecution methods used. Apart from definitional issues, computer-related crime involves crossing boundaries and borders not seen in traditional crimes. However, Stephenson (2000) argues that computer-related crimes do not always equate with traditional descriptions of illegality. Some activities in computer-related crime present unique forms of criminal conduct that bear no conformity to common law or existing crimes. For example, computerization allows for new types of crimes, such as trafficking in passwords.

Tavani (2000:7), with a different opinion mentions that other computer-related crimes may have conformity to traditional crimes but the conduct may not fit neatly into an existing category. For example, theft of an ATM card and subsequent transaction from the ATM may be both theft and fraud or electronic fraud. It is challenging to ascertain whether this conduct fits within theft or fraud cases. According to Alkaabi (2010:15), computer-related crime legislations are enacted to cater for these new forms of criminal conduct. The aptitude of the Internet provides accessing information with obscurity making crimes, such as identity theft, important priorities for the legislators.

The researcher noted that, in traditional crimes there is usually traces of evidence such as, deoxyribonucleic acid, (DNA), footage recorded on surveillance cameras, fingerprints, photographs and, or suspects personal identification

2.14 WAYS IN WHICH COMPUTER IS USED IN CRIME

According to Cohen (1991:4), computer is defined as “any apparatus or device, whether or not called a computer and which is capable of capturing and absorbing data supplied to it through electronic, electro-mechanical and mechanical.” It processes such data according to mathematical or logical rules and in compliance with such instructions of storing such data before or after such processing. The computer is also able to produce information obtained from the data as an end product of such processing. Barata (1999:5) agrees with Cohen (1991:4) and in a simplified definition says a computer is a machine designed to perform a desired sequence of operations and capable of storing of information which is then processed to carryout functions such as organising words and calculating numbers. Coelli (2008:37), splits the definition into two elements although embracing discussions by Cohen (1991:4) and Barata (1999:5) and summarizes that a computer is an electronic gadget capable of accepting, storing, and logically manipulating data or text that input and processing and producing output on the basis of stored programs of instructions. Microsoft Computer Dictionary (2002:118) mentions that a computer is any device capable of processing information to produce a result that is desired and achieved through accepting input, processing the input as well as producing output. In order to understand how computers can be used to commit crime, there is a need to understand computer system, which Cohen (1991:4), defined as “an electronic, electrochemical optical, magnetic, or other data processing device, including its physical components, and any removable storage medium or a group of such interconnected or related devices capable of containing data, or performing a logical, arithmetic or any other function in relation to data.”

According to Cohen (1991:4), data is defined as “electronic representations of information in any form.” Saboohi (2006:3) illustrates that a computer can be used to commit crimes where a computer is the target for crimes such as hacking, or where computers are the means by which criminal acts are executed such as software piracy and internet frauds. There are also crimes, as further argued by Saboohi (2006), where the use of a computer is consequent to criminal acts, for example; storing information on a computer about drug trafficking and white collar crimes.

Participants were asked to explain the main ways in which a computer can be used in crime and nine participants in sample A said the computer can be the object of the crime or the instrument with which the crime is committed. Fourteen participants from sample A indicated that a computer can be an object of the crime, repository of evidence and used to commit the crime. Seven participants from sample A had no idea. Icove, Seger and Vonstroch (1995:62), look at ways in which a computer is used to commit crimes and list them as follows:

- Computer trickery crime- is committed by a person for self-gain or injuring the person of another through data transfer or by inputting misleading data or deliberate omission of data so that electronic processing results are changed.
- Financial theft and misuse crime- committed with use of computers, for example, the misuse of credit cards or access into the protection systems to make unauthorized financial transactions. The computer may also allow forgery of data in electronic form and documents in legal traffic such as bank notes through scanners and printers.
- Computer viruses crime- through software programs designed to cause damage to many computers connected in network. The viruses copy themselves into each computer they come in contact with and are not noticeable unless a program for virus scanning is installed. The attackers delete useful data or send data to other location in the network.
- Computer espionage access of government network means to perform a modern form of intelligence. Industrial espionage is used for commercial purposes.
- Computer sabotage crime is where suspects destroy, delete, change, hide or make datum or program useless or damage the computer which is important for a state organ, institution or public service.
- Hacker ship crime is committed by decoding and breaking the protection of an information system with an intention to enter it.

Olufunke (2010:4) agrees with Icove et al. (1995:62) that the use or access to computer or its components is an essential element. Computer crime cannot be committed without

the use of a computer. The use of the computer also ranges from unauthorized access or accesses exceeding authorization to computer systems, data alteration or data destruction including theft of intellectual property. The hacker breaks into a computer to steal or to bypass password and other security features, the intention being to commit financial fraud or to steal some sensitive data. Olufunke (2010:4), further mentions that if the crimes targeted are networks, the connectivity of computers increases the number of prospective victims of computer-related crime and creates wider opportunities to criminals. Tubake (2013:118), shares the same opinion with Olufunke (2010:4) that the definition of computer-related crime emanates from the use of a computer as an instrument to commit crimes such as fraud, child trafficking, intellectual property, violating the piracy, pornography, theft and identity.

According to Alkaabi (2010:83), the computers are used in the commission of crimes, the first being in crimes where the computer, computer network, or electronic device is the primary objective of the criminal activity and are in four sub-types namely:

- Unauthorised access crimes such as hacking.
- Malicious code crimes such as the dissemination of viruses and worms.
- Interruption of services crimes such as disrupting or denying computer services and applications, for example, denial of service attacks and botnets.
- Theft or misuse of services: examples of theft or misuse of services include theft or misuse of someone's internet account or domain name.

The second group include crimes where the computer, computer network, or electronic device is the tool used to commit or facilitate the crime and are in three sub-types listed as follows;

- Content violation crimes such as the possession of child pornography, unauthorized possession of military secrets and IP offences.
- Unauthorised alteration of data, or software for personal or organisational gain such as online fraud.
- Improper use of telecommunications such as cyber stalking, spamming and the use of carriage service with the intention or conspiracy to commit harmful or

criminal activity. It also covers social engineering fraud such as phishing and scare ware.

The researcher noted that, regardless of these crimes being traditional crimes facilitated by computer systems, the emergence has created new dimension because their physical proximity is no longer intrinsic to commit traditional crime. The criminal capability is now amplified to commit the crime anonymously, and without leaving a single trace. The computer system helps the crime to occur faster and makes it harder to trace and investigate.

2.15 CLASSIFICATION OF COMPUTER-RELATED CRIME

The classification of computer-related crime is drawn from the definition of computer-related crime. Alkaabi (2010:9), proposes an integrated extensive classification of computer related crime by dual characteristics of the role of the computer and the contextual nature of the crime. Icove et al. (1995:63), sectored computer-related crime in four categories guided by the modus operandi as well as the method of attack and prevention methods being the major elements. They listed them as; breach of physical security through physical action, breach of personal security, breach of communication and data security, and breach of operations security. Tubake (2013:129) classifies computer-related crime into a cluster of four, thus; crime against Individual through computers or networks, for example, in e-mail spoofing, phishing and spamming, or crime against property of a person, for example, credit card skimming, Intellectual property crimes, internet time theft and identity theft, or crime against organization and includes banks or service sectors, for example hacking, denial of service, virus and worms and spywares and finally, crime against society such as pornographic websites, illegal internet auctions, terrorist activities, and terrorist activities through use of computers, counterfeit notes and revenue stamps.

When asked what the classification of computer-related crime is, two participants from sample A suggested that computer-related crimes are classified according to the type of the crime, victim and motive of the suspect and six participants from sample A, indicated

it is governed by the role of the computer; this is affirmed by Alkaabi (2010:18). Twenty-two participants from sample A, said they had no idea. Participants did not have an opinion on this question even though the researcher felt they had much to add. The participants opted to making questions instead. According to Gordon and Ford (2006), as *cited* by Ngafeeson (1999), computer-related crime is viewed as either computer-assisted or computer-focused. The technological crimes fit into the category of computer-focused crime while those that are people-related are in the category of computer-assisted crime. These classifications are closely related. Alkaabi (2010:18), sees differences in that specific crimes are encompassed by the terms computer related crime and classifies them into three categories:

- The use of a computer as a target of criminal activity (e.g., hacking, dissemination of viruses)
- The use of a computer as a tool or instrument used to commit a criminal activity (e.g., online fraud)
- The use of a computer as incidental to the crime (e.g., data storage for a criminal activity)

However, still others classify computer crime or cybercrime into only two categories, thus, crime that is committed using computers and networks for example, hacking and viruses and traditional crime that is facilitated through the use of computers such as child pornography and online fraud. Alkaabi (2010:16), supports the view of categorizing the classifications of computer related crime by Ngafeeson (1999). Alkaabi (2010:16) further identifies two main types of computer crime or high-tech crime, the first type being crimes where the computer is a target of an offence, for example, hacking, terrorism; and crimes where the computer is a tool in the commission of the offence, for example, online fraud, identity theft. In addition, Alkaabi (2010:19) elaborates that the second type is where the computer is a tool, based upon the level of reliance on technology such as computer-enabled crimes, computer-enhanced and computer-supported crimes. Other classifications have elaborated on the above in one way or another. However, despite some considerable differences, there is a core of consistency between some of the above classifications. It is becoming increasingly accepted that the computer system plays two

main roles in computer-related crime as a target of a criminal activity or as a tool to commit a criminal activity.

The researcher concurs with the aforementioned view. In contrast to the above computer-related crime classifications, there are other classifications some of which include consideration of factors other than the role a computer system plays in the committing of computer-related crime. These factors include: threats, attackers, and victims. Kadir (2010:615) says computer-related crimes are classified in two categories, firstly being,crimes where a computer system itself is the target such as hacking, dissemination of viruses, denial of service attacks, traditional crimes like fraud, theft, and child pornography that are facilitated and enabled by a computer. In second classification, he categorizes computer crimes into four types, namely, theft of money, financial instruments, property, services, or valuable data; unauthorised access to computer time; illegal use of computer programs; and unauthorized acquisition of stored data.

Researcher has noted that computer crimes are classified according to the computer's role in the commission of the crime first, with the computer being the object and secondly, subject of a crime or the instrument used for perpetrating traditional crimes. It is worth noting that, according to Icove et al. (1995:64), in analysing the foregoing classification of computer related crime, discussions were on modus operandi where such crimes as malicious injury to hardware caused by breaching of physical security or personal security cannot be prosecuted as computer-related crime. On a different opinion, Schell and Martin (2006:115) sectored computer-related crime into two categories being (i) harm to property and (ii) harm to a person.

2.16 INVESTIGATION OF COMPUTER CRIME SCENE

According to Baber, Smith, Panesar, Yang and Cross (2006:3), crime scene investigation commences with an incident that is interpreted as criminal. The investigation proceeds through examination of a scene, to the selection, collection and analysis of evidence. It relates the evidence to a criminal case that can be answered. Yusoff, Ismail and Hassan (2011:20), explain that computer related crime scene is a virtual environment established

through software and hardware where digital evidence of a crime or incident exists. Collier and Spaul (1992:316) whilst agreeing with Baber et al. (2006:3) and Yusoff et al. (2011:20) mention in their discussion that in the computer context the scene of crime and the location of the perpetrator may vary due to network computing. This makes it difficult to link the physical evidence to the suspect. However, it is possible to link electronic evidence established through electronic trail to a device and reconstruct and extract evidence from computer files. Wori (2014:52) explains that computer-related crime adhere to "Exchange Principle", in that the suspect leaves some form of evidence at the scene and takes away some form of evidence which links them to the crime. However, at times the actual location of scene poses a challenge because of the disconnectedness that the Internet provides. This creates a physical separation between the actual crime scene and the perpetrator.

According to Cyber Crime Investigation Manual (2011:28), computer-related crime scene is entirely diverse from the traditional conventional crime scene mainly because of the fragility of digital evidence and its vulnerability to interventions. It calls for utmost care and precautious handling during search, retrieval, transportation and examination. Cyber Crime Investigation Manual (2011:28) discusses the sequential steps for approaching the computer-related crime scene as follows:

- Identifying and securing the crime scene
- "As is where is" documentation of the scene of crime
- Collection of evidence
- Procedure for gathering evidences from switched-off systems
- Procedure for gathering evidence from live systems
- Forensic duplication
- Conducting interviews
- Labelling and, documenting of the evidence
- Packaging, and transportation of the evidences

Participants were asked on how they will approach computer crime scene and fourteen participants from sample A mentioned that the approach to the computer crime scene should consist of planning and securing the scene, documenting the scene, photographs and a search for computer evidence. Eleven participants from sample A, stated that computer-related crime scene is similar to a traditional crime scene and should be approached by initially assessing the scene, searching for physical evidence, documentation before any collection of evidence is done, preservation of evidence and reconstruction of the scene. Five participants from sample A, posited that, approaching computer-related crime scene entail securing the crime scene from unauthorised access by others, to eliminate contamination before evidence is collected. The foregoing responses by the participants are further discussed in Cyber Crime Investigation Manual (2011:28) and by Collier and Spaul (1992:316).

Cyber Crime Investigation Manual (2011:28), discusses the preliminary investigation of the scene of computer-related crime and adds that the investigators should survey the scene regardless of whether it is an individual's home with one or more computers, cyber café or public places or companies with more computers coupled with complicated networks. The pre-scene investigation will aid the investigators in familiarizing with the local set up, circumstances, technical details of the systems and networks at the scene of crime. Digital evidence is located in divers' devices and divers' formats such as in the copiers, fax machines, routers and hubs, amongst others. This also equips the investigator with added steps to identification of evidence, conducting a search and as well as notes that are sent to Forensic Science Laboratory (FSL) for expert opinion. Cyber Crime Investigation Manual (2011:28) further illustrates that it is a matter of good practice for the investigator to video graph, photograph, draw the network architecture sketch in "as is where is" condition of the crime scene and document it.

According to Cyber Crime Investigation Manual (2011:27), and Collier and Spaul (1992:316), the procedures at the computer-related crime scene are listed as follows:

- Following the identification of scene of computer-related crime the investigator should secure and note every person present at the scene of crime and their roles.
- The investigator should identify all the potential evidences including conventional physical evidences like the manuals, user guides, passwords on slips and bank account numbers. It will also be ideal to note the position of the various peripherals at the scene of crime. For example, left handed person will leave the mouse on the left hand side of the desktop.
- The investigator should identify all the perishable evidences and arrange for preservation without disturbing or altering the condition of electronic evidences.
- The system that is already OFF should not be turned ON. If systems are on, they should be left ON.
- On systems that are ON, the investigator should photograph them and document them before technical personnel assists in seizing the evidence.
- The investigator should note all the attached network cables and power lines to the systems and all the network connections, modems, telephone lines and, mark the equipment connection from end and from the source in the walls.

Cyber Crime Investigation Manual (2011:28) explains that preliminary interviews at the scene of crime will aid the investigators to identify potential evidence during pre-Investigation. The investigator may ask the following questions.

- Steps taken to contain the crime such as denial of physical access to suspected persons and disconnecting their computers from network.
- If there are any logs such as access to the system access and suspicious entries.
- Information on anyone who used the system after the crime occurred.
- Notifications by the firewall, Intruder Detection System (IDS) and network security devices.
- Log registers of users.
- Identification of complainant or owner(s) of the various devices and obtain the access details, usernames, service providers' details.

- Information on all the security systems such encryption policies and, off-site data storage, data centre and disaster recovery policies of the organization or back-up plans.
- Identification of the people familiar with the network and a schematic diagram of the network.

Cyber Crime Investigation Manual (2011:31) prescribes that in the pre-investigation technical assessment the investigator is equipped with the idea in the number of computers, the number connected to internet, the network topology and architecture. This will include details of other computer peripherals. Pre-investigation also assists in containment of the crime and reduces alteration of evidences crucial in successful prosecution. Shinder (2002:553) agrees with Collier and Spaul (1992:316) and adds that when approaching the computer related crime scene the first participants should not attempt to shut down or unplug the computer or access it to look for evidence as this may alter or destroy evidence. At the computer-related crime scene the first participants should do the following:

- The investigator should identify the scope of the computer related crime scene before putting a perimeter and compile list of systems involved in the criminal incident and from which evidence will be collected.
- In protecting the computer-related crime scene where digital evidence is sought the entire systems should be considered part of the crime scene regardless of whether they are powered or not functional. This includes laptops, notebooks, and other portable computers. It will be ideal to sustain a cordoned off scene.
- There should be preservation of temporary and fragile evidence by recording it and taking photos of screens.

Shinder (2002:553) and Stephenson (2000) are of the opinion that in approaching the scene, the investigator is responsible for coordinating all the activities at the scene and that includes:

- Ensuring that all critical decisions are filtered through the investigator, including the moving or accessing of computers and related equipment until collection of evidence has been done.
- The investigator directs the crime scene search on computer hardware, software, manuals, written notes, and logs related to the operation of the computers. This includes printers, scanners, and all storage media: diskettes, optical discs, tapes, and other removable disks, and any "extra" hard disks in the vicinity.
- The investigator should protect the computer-related crime scene whilst preservation preparations are made. The investigator oversees the actions of the crime scene technicians and conveys considerations that should be taken based on the nature of case and knowledge of the suspect(s).

2.17 INVESTIGATION MODELS DEVELOPED BY COMPUTING EXPERTS

Traditional forensic experts and technologists developed technical implementation of the investigation process to address computer-related crime. They introduced models to capture the complete scope of an investigation process. A good investigation model of computer-related crime will provide an abstract reference framework without the influence of technology. This assists in the discussion of techniques and technology that support the work of investigators. When asked of the investigation models developed by computing experts, all the thirty participants from sample A expressed a knowledge gap as they were not familiar with the models. According to Perumal (2009:39), in addressing the existing digital forensic investigation model, described computer forensic as an application of methodical technique to investigate computer-related crime. Existing model produced three phases that is; acquiring, authenticating and analyzing evidence. Ciardhuáin (2004) stressed that a computer-related crime investigation existing model aids in developing new techniques and tools for investigators. This model besides processing evidence depicts the information flows in an investigation thereby taking cognizance of the entire computer-related crime investigative process including the digital evidence processing activities. Kohn, Eloff and Olivier (2006) in discussing Lee's Model of Scientific Crime Scene Investigation concludes, it is biased to scientific crime scene

investigation and as such does not include full investigative process. It identifies four steps within the scientific crime process:

Recognition is the initial step in which items or patterns are viewed to be potential evidence and subsequently lead three sub-activities comprising of collection, preservation and documentation. Identification of the divers' of types of evidence is the second step and deals with classification of evidence with only one sub-activity and comparison to known standards. Individualization in determining unique evidence with possible links to events or individuals. Reconstruction in putting together a series of parts of the process that constituted the crime. The results activate reporting and presentation.

Lee's Model of Scientific Crime Scene Investigations encompasses and describes logic tertiary for divers' types of scenes. They ensure, evidence is identified, individualized and reconstructed by guiding investigators appropriately through systematic and methodical investigation. Lee's Model of Scientific Crime Scene Investigations is somehow biased towards use of physical evidence but as the discussions broaden it will depict that it is also related to electronics scene as well (Kohn, et al. 2006).

According to Ciardhuáin (2004), Casey's model is for processing and examining digital evidence and its steps are; recognition, preservation, collection, documentation, classification, comparison, individualization and reconstruction. These steps are similar to Lee's Model of Scientific Crime Scene Investigation as discussed by Kohn et al. (2006).

In the Casey's model, evidence is analysed in the last two steps because the reconstruction usually points to additional evidence which may ignite the cycle to restart. This is so because the model is firstly viewed in standalone computer systems, followed by application to the various network layers and subsequent description of investigations on computer networks. Casey's model is applicable to both standalone systems and networked environments (Kohn, et al. 2006).

Ciardhuáin (2004) mentions that the first Digital Forensics Research Workshop (DFRWS) produced a model which prescribed sets for digital forensic analysis in a linear process and listed the steps as: identification, preservation, collection, examination, analysis, presentation and decision. Whilst the foregoing model was not adopted as a final comprehensive one, it set a tone for future work and research. The DFRWS model is linear and feedback from one step to previous ones is possible. However, it does not discuss the steps of the model in great detail, but limits the discussion to time synchronization, imaging technologies, case management and chain of custody. Ciardhuáin (2004) describes a model derived from the DFRWS in nine steps, thus, identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation and returning evidence.

Yusoff et al. (2011:18) say the Digital Forensics Research Workshop (DFRWS) 2001 proposed a general purpose digital forensics investigation process comprising of 6 stages and this is less two stages in the form of returning service and approach strategy as asserted by Ciardhuáin (2004). Reith, at al. (2002:8) drawing their inspiration from DFRWS investigative model went on to propose an enhanced model known as Abstract Digital Forensic Model and they introduced three more phases, expanding the phases to nine. The 3 phases brought along to the model are preparation, approach strategy and returning evidence. In preparation issues relevant were getting tools ready, identification techniques and other supporting activities were done. Approach strategy was introduced to ensure acquired evidence was not tainted and held so until returned safely to the owner. This also encompassed the returning evidence phase (Ademu, Imafidon and Preston, 2011:176).

Ciardhuáin (2004) and Kohn et al. (2006) suggest this model is also effective if used to investigate fixed hard drives or embedded non-volatile memory in identifying familiarities in procedures or tools. Ciardhuáin (2004) points out that the existing models do not cater for all aspects of computer-related crime investigation as their focus is on the processing of digital evidence. The existing models cannot aid any development of new investigative

tools and techniques. The other limitation with the existing models is that they concentrate on the middle part of the process of investigation, thus in collection and examination of the evidence. According to Yusoff et al. (2011:20) Integrated Digital Investigation Process (IDIP) 2003 was proposed by Carrier and Spafford (2003), with an aim of combining divers' available investigative processes into one integrated model. Ademu et al. (2011:176) states in this model that the concept of digital crime scene which refers to the virtual environment created by software and hardware where digital evidence of a crime or incident exists is introduced.

Yusoff et al. (2011:21) says in 2004 Enhanced Digital Investigation Process Model (EDIP) was introduced based on the Integrated Digital Investigation Process (IDIP). It brought aboard the trace back phase to aid the investigators to trace back to devices and computers used by suspects in the commission of the crime. Yusoff et al. (2011:24) emphasize that Computer Forensics Field Triage Process Model (CFFTPM) was introduced in 2006 and it proposed an onsite approach in the analysis, identification and interpretation of digital evidence without forensic images. It has six primary phases and six sub phases. Ciardhuáin (2004) says a compressive model should flow through the following:

- Awareness- allows the relationship with the events to be investigated to clear.
- Authorisation- authorisation setting out what is permitted in an investigation.
- Planning- guided by regulations and legislation prescribing the general context of the investigation and which are not under the control of the investigators.
- Notification-informing the subject of an investigation.
- Search for and identify evidence- location of evidence and identification of the next activity.
- Collection of evidence- assuming possession of the evidence in a form that can be preserved and analysed.
- Transport of evidence- physical transfer of seized computers and transmission of data through networks.
- Storage of evidence- preserving the integrity of evidence.

- Examination of evidence- use of techniques to find and interpret significant data.
- Hypothesis- preparation of hypothesis with supporting material from the examination for use in court.
- Presentation of hypothesis- hypothesis will be placed before a court.
- Proof/Defence of hypothesis-proving the validity of the hypothesis and defending it against criticism and challenge in court.
- Dissemination of information- dissemination of information from the investigation that will influence future policies and procedures.

Ciardhuáin (2004), says investigation through the foregoing model proceeds in a "waterfall" fashion with activities following each other in sequence through the investigation process. These activities allow back tracking. At the same time a chain of custody is formed through the list of those handling evidence and they are added to each step. Ciardhuáin (2004) and Ademu et al. (2011:176) agree there is information flow in the model. Firstly, from one activity to the next to provide support in the form of automated procedures and tools such case management tools. Authorization allows further information flows to and from the appropriate authorities. The planning takes cognisance of policies, regulations and legislation which govern how the investigation can proceed and the hypothesis on the evidence must be justified in court. On completing of investigation there is information flow following dissemination of results. In an abstract model it is not possible to identify clearly all the flows.

Shin (2011:6) and Kohn et al. (2006) corroborate in their discussion of a new model for computer related crime investigation procedure that it should consist of the following:

- readiness phase,
- consulting with profiler,
- computer related crime classification and investigation priority decision,
- damaged computer related crime scene,
- analysis by crime profiler, suspects tracking,
- injurer computer related crime scene investigation,
- suspect summon,

- computer related crime logical reconstruction,
- Writing report.

Shin (2011:6) is optimistic that if the investigators apply it to the actual investigation the presented procedure will be effective.

2.18 SUMMARY

The investigators should understand the nature and the impact of computer-related crime, its investigation and the challenges encountered in the process. The investigators should be able to analyse and determine whether a crime has taken place and how to handle a computer-related crime scene. The investigators also need to understand the laws that are applicable to prosecution of computer-related crime as this will guide them in collecting and preserving electronically-based evidence. In the next chapter 3, the researcher will be discussing procedures for searching evidence in computer-related crimes.

CHAPTER 3: THE PROCEDURES FOR SEARCHING EVIDENCE IN COMPUTER-RELATED CRIMES

3.1 INTRODUCTION

Computer-related crime evidence is very diverse and it ranges from the computer mainframe, to pocket-fit personal data assistant, to the floppy diskette, the minute electronic chip device or CD. It is also volatile and as such images, audio, text and other data on these media can easily be altered or destroyed. In view of the foregoing, investigators are expected to adhere to best practices and guidelines for searching of computer- related evidence. In any case, the objective is to obtain evidence that will be admissible in court and is not subjected to inadvertent alteration or destruction.

In this chapter the researcher will discuss the concept of search, software tools that can be used in searching evidence during the investigation of computer crime, the standards or legal requirements for searching and preserving computer evidence, if traditional searching procedures applicable to physical objects also apply to the intangible objects. Basic strategies and procedures for searching computer evidence, if information that has been retrieved through software tools can be accepted as evidence during trial, the importance to maintain chain of custody when collecting and preserving computer crime evidence, will also be focused. The chapter will conclude by focusing on the use of computer forensic expert to search and preserve computer evidence, the legal requirements for the admissibility of computer evidence in court, how computer evidence is presented in court and the challenges faced by investigators in dealing with computer evidence.

3.2 CONCEPT OF SEARCH

According to Meeker (2005:6), search occurs if the immanent act of the mind of a person's apprehension of privacy is violated. Meeker (2005:6) further explains that the violation is actually done by Government and quotes Kyllo v. United States, 533 U.S.27, 121 S.Ct. 2038 (2001) where the court proscribed use of thermal imaging device without a warrant. The definition of "search" was protracted to encompass procuring information by sense-enhancing technology regarding the interior of a home that could not contrarily have been

retrieved without a physical intrusion into the home. Jarrett and Bailie (2009:28) agree with Meeker (2005:6) that a search occurs when an anticipation of privacy that society regards reasonable is transgressed. A search is, therefore, viewed as constitutional if it does not infringe a person's reasonable or legitimate apprehension of privacy. Sady (2012:4) argues that the definition of a search has significant exceptions contracted by an increasingly narrow view of anticipations of privacy deemed reasonable. For example, visual observations into the interior of a home may constitute a search or requiring a person to open a door so that the investigator has visual access of the interior of the house may constitute a search, even if there is no physical entry.

The participants were asked to define the concept of "search" and thirteen participants from sample A pointed out that a search is done to find items or information that will aid in finding a solution to a criminal case. Nine participants from sample A indicated that a search is to examine another's premises with legal authority, to seek for evidence related to criminal activities. Eight participants from sample A described a search as a process of looking for something that has to be used in a court of law to prove a criminal case. Three participants from sample B highlighted that a search is an examination of evidence under the authority of a search warrant or conducted by a person who on probable cause believe there is evidence on the premises, but there is no time to get a warrant. The rights to privacy enshrined in the Constitution should not be violated as they render evidence illegal if they are breached. The researcher shares the same views with Meeker (2005:6) and three participants from sample B that a search is an examination of premises by investigators seeking for evidence to prove a crime has been committed. The search has to be reasonable and within the confines of the law. It should not violate the rights of the occupants.

Eleven of thirty six dockets perused show on the running diary logs Zimbabwe Republic Police form (ZRP) 11 that searches were done but do not indicate the methods on how they were done although the recovered items are listed on the reverse of the crime report forms (ZRP) 66 and (ZRP) 17. There are defined methods of carrying out the crime scene

search. According to Miller (2011), the preliminary crime scene search is usually done to establish physical evidence and orientate it before resorting to documentation. Miller (2011), illustrates as a safeguard to ensure no evidence is lost, that search methods have been developed and no single search method is relevant to specific types of scenes. Miller (2011), further stresses that search methods used are geometric six patterns consisting of;

- Link method that seek to link the victim, physical evidence, and the scene to the suspect.
- Line or strip used to search a vast area for a large object. The searchers stand in single long line and all walk the same direction using a rope to create lanes for which each searcher would be responsible.
- The grid search is simply two parallel searches performed one after the other at 90 degrees.
- In a zone search, the crime scene is divided into sectors and each sector allocated to each member. Team members switch sectors and search again to ensure complete coverage.
- wheel or ray, a method employed by several people moving from the boundary straight toward the center of the scene (inward) or from the center straight to the boundary (outward).
- Spiral used for searching for an object that is suspected to be at a specific distance from another.

Miller (2011) notes that, in certain crime scenes the search methods may be combined although they should not interfere with each other. Law Commission Report (2007:198) states that the methods used to search conventional crime may not be applicable to computer-related crime and discuses that computer searches can be conducted in divers' ways such as;

- Accessing data directly on the target computer and printing out or copying to disk any evidential material for removal.

- The use of write-blocking devices to preview data on the target computer. These devices allow a direct search of the data, but quarantine it to preserve its evidential integrity to allow Investigators or forensic analysts to copy evidential material;
- Taking and searching a forensic copy of the hard drive of the target computer, rather than searching the hard drive directly thereby preserving the evidential integrity of the data.

Texas Explorer's Guide to Law Enforcement Training Manual (2012:14) groups the initial scene searches in three categories, thus; hot search; a high risk response to a suspect still at the scene, cold search; done some considerable time after the scene was discovered and an organized approach. In the organized approach the following are ensured; the search is conducted thoroughly and it is legal, the search is done without compromise and expeditiously, the scene is documented properly, evidence recovery is done through appropriate methods and techniques, equipment and resources are properly used by knowledgeable persons, evidence recovered is pertinent, handling and packaging of evidence is done properly, there are appropriate distribution points for evidence analysis and that safeguards are observed. Texas Explorer's guide to law Enforcement Training Manual (2012:14) emphasizes that, for objectives of searching to be achieved, there should be a searching team leader who will coordinate the activities of other members and their responsibilities. These include photographer, photographic log recorder, sketch preparer, evidence recorder and custodian. Meeker (2005:6) suggests that after the search it will be prudent to release the scene.

3.3 SOFTWARE TOOLS USED IN SEARCHING FOR COMPUTER-RELATED CRIME EVIDENCE

According to Pladna (2008:6), computer data searched is presented in two types, thus persistent data stored in a hard drive or similar medium and is retained even if the computer is switched off and, secondly, volatile data stored in a Random Access Memory (RAM) or it is in transit and can be infringed if the computer is turned off. Maras (2011:192) suggests that, in such live responses, Universal Serial Bus (USB) can be used to collect

searched volatile and non-volatile from live systems before they are shut down. In view of the foregoing Pladna (2008:6) further notes that the tools used for searching computer-related evidence should possess divers software in the form of backup, decryption, authentication, log file auditing, disk editing, IP tracking, file examination and data recovery.

The participants were asked to name software tools that can be used in searching evidence during the investigation of computer crime. Notably, thirty participants from sample A and three participants from sample B were not aware of the searching software tools used for searching computer-related crime evidence. The researcher observed that the participants have not been exposed to searching software tools. The participants were aware of the traditional investigative techniques as they relate to advanced technology, and seemed overwhelmed by technology in relation software used to search evidence. The researcher further questioned the participants on their knowledge on the availability of technology that may enhance the investigation or provide information that may not otherwise be available to the investigator. Whilst they seemed aware, they could not answer the question and list software that may assist in searching and identification of evidence. Pladna (2008:7) and Scientific Working Group on Digital Evidence Version (2006:06) in their discussion are of the opinion that hardware imaging tool should be used to copy data bit by bit using a bit-stream-copy method. Anti-cartel enforcement manual (2010:11) acknowledges a bit stream imaging software creates an image of all areas of a data carrier making a mirror copy of each bit contained therein. Maras (2011:189) states that the backups will then copy all data from the hard drive except ambient data located in the swap file which acts like a memory of a windows system. Maras (2011:192) further explains that ILook can also be used to search computer media thereby imaging and retrieving deleted files including email analysis. Pladna (2008:7) and Maras (2011:191) agree that in the searching process the hardware imaging tool will duplicate a bit-stream or an image of an original disk or section without altering original evidence, verify the integrity of a disk image file, log and fix errors. The software operation will ensure the output of the recorded documentation is correct.

Pladna (2008:7) and Maras (2011:190) further mention that Authentication software ensures that the originality of evidence is sustained by using programs in the form of Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1). These are capable of producing encrypted hash codes. Schatz (2007:139) and Kozushko (2003) add MD5 through implied mathematical calculation method saves the data to the drive or document.

According to Pladna (2008:7), decryption tools aid access to password protected computers, files and cipher text back into plain text. This can be achieved by guessing the password and using a system vent or a high speed computer with decrypt software if the password is protected on boots up universal. Sommer (2013:95), mentions that another approach is to use dictionary attack where a list of passwords in large numbers is thrown into encrypted file until the appropriate password is established. According to Maras (2011:179) and Schatz (2007:157), Basic Input Output System (BIOS) password can also be used or by clearing Complementary Metal Oxide Semiconductor (CMOS) to return setups to default. A jump on the motherboard may be used or alternatively the battery removed. Pladna (2008:7) points out screensavers, documents, Portable Document Format (PDF) files, and compressed files contain programs that can aid the breaking of passwords. Dahake and Daware (2012) in their discussion say another code-breaking and password recover called Forensic Tool Kit (FTK) can be used. They argue that it is advanced compared to other software because it can provide both Page and E-mail Support as it is loaded with Unicode and has strong search functionality.

Pladna (2008:6) notes deleted data does not leave the hard drive and this information can be traced using a disk editing and searching tool such as Winhex Editor Program with capabilities of searching for strings of code on the hard drive for identification of relevant data. Ambhire and Meshram (2012:394) and (Sommer 2013:54) are of the opinion Prodiscover is another method that can be used to establish data on a computer disk without evidence interruption or Helix3Pro that can be used on multiple operating systems such as Windows, Macintosh and Linux has safeguard against alteration of data during

imaging (Maras, 2011:191). Pladna (2008:6) stresses that the daily audit log file tool replicates the event monitor on Microsoft Windows computer and; according to Sommer (2013:110), Intrusion Detection Systems (IDS) are equipped with a daily audit file that records the identity using cookies of who logged on and off and whether the files have been altered or deleted including browsing from the internet. Pladna (2008:6) agreeing with Kent, Chevalier, Grance and Dang, (2006:17) illustrate upon entry into the computer's operating system, other tools can be used, for example; the use of a ping command on a Windows based computer to track an IP address and two pieces of other software, Whois and trace-route provide further information on the IP address.

Pladna (2008:7) and Kent et al. (2006:17) opine that an R-Mail tool is used to recover messages where messages are hidden, whereas Craiger, Swauger and Marberry (2005:06) indicate steganalysis can be used to detect steganography software which hides messages and data. Pladna (2008:6) and Forensic Examination of Digital Evidence, A guide for law Evidence, (2004) mention a Quick View Plus is used to read document with divers file formats. Maras (2011:191) and Schatz (2007:51) underpin Encase is used to create the drive's image without altering its contents and calculates the hash value for further authentication making it able to locate hidden partitions and files within the same drive. Forensic Examination of Digital Evidence, A guide for law of Evidence, (2004) and Ambhire and Meshram (2012:394) reiterate that Encase has the ability to search multiple locations and devices at the same time. The foregoing Encase functionality has immediate response capabilities thereby eliminating system downtime (Dahake and Daware, 2012).

The researcher's understanding is that the software and tools discussed by the foregoing authors explain how to search for computer-related evidence and the methods of how to deal with particular evidence such as authentication, backing up data, file auditing, decryption, data recovery, IP tracking and examination of document. A digital evidence bag (DEB) is used to store information obtained from divers' applications.

3.4 STANDARDS OR LEGAL REQUIREMENTS FOR SEARCHING AND PRESERVING COMPUTER EVIDENCE

Kerr (2005:85) defines search warrant as a compelling power authorizing investigators whilst observing the rights of citizens to enter into a location to search evidence of crime. Meeker (2005:29) defines a search warrant as a document that authorises search for discovering things relevant to an investigation in a private place. Smith and Hartmann (1998) point out that it is a written document in which the judicial authorises investigators to enter and search a specific place for specific articles and to seize those articles that form evidence to the crime once found. Duhaime (2005) commenting on the matter of A.G. (Nova Scotia) v. Macintyre, [1982] 1 S.C.R. 175 describes a search warrant as a document used to search a private place for evidence. Perlmutter (2013) defined a search warrant as an order signed by a judge or a magistrate that authorises investigators to search for specific articles, at a specified location and at a defined time. Perlmutter (2013) depicts three aspects of a search warrant, thus, specificity of the items to be sized, the location and the time of the search execution. The search warrants defined above are relevant to the search of tangible items which means there is need to define computer-related crime search warrant separately.

Eleven participants from sample A were asked what were the standards or legal requirements for searching and preserving computer evidence and indicated that, the legal requirements are to ensure that, an unreasonable search does not occur, any evidence seized as a result of it would not be admissible in a criminal prosecution. Twelve participants from sample A posited that, legal requirements are safeguards from police arbitrary intrusions, whilst seven participants from sample A mentioned “the fruit of a poisonous doctrine”. Three participants from sample B said, the standards and legal requirements ensure, either the police must have probable cause, or they must have reasonable suspicion The participants seemed guided by section 47 of the Zimbabwe Criminal Procedure and Evidence Act 14 of 2004, that a search warrant is a document issued by a judicial officer or justice of peace to search articles used in the commission of a crime. The researcher noted that, whilst the participants may be somewhat aware of the standards and legal requirements, their lack in detail made them refrain from

expressing their knowledge. The eleven out of thirty six dockets in which searches were done did not contain any search warrants or consent to search records. The information on the running diary log ZRP form 11 highlighted that searches were done and the property recovered consisting only of computers and their peripherals listed. There was silence on how the searches were conducted.

According Feltoe (2009:20), there is no instruction for issuing of computer related crime search warrant. Investigating officers must obtain a conventional warrant to search computer-related crime location following a presentation of an affidavit either to a judicial officer or to a justice of the peace. Feltoe (2009:20) further explains that the premises to be searched must be precisely described and the items to be searched for must be specifically stated. In the *Capital Radio (Pvt) Ltd v. Minister of Information & Ors (2)* 2000 (2) ZLR 265 (H), it, was held that, “the warrant issued by the magistrate was invalid as it contained two serious flaws. Firstly, the warrant purported to be applicable throughout the country, whereas a magistrate only has jurisdiction to issue a warrant in respect of his area of jurisdiction. Secondly, the warrant was far too broad and vague and was lacking in specific detail. The warrant did not specify the premises to be searched, neither did it state the reason for the search”. Mussio (1990:88) is of the opinion that there should be probable cause, which means the person issuing the warrant should be satisfied that there are reasonable grounds for carrying out the search. There should also be reasonable basis for believing that the search will lead to the seizure of items used to commit a crime or provide evidence of the commission of a crime. Mussio (1990:88) further augments that this is achieved by establishing that; a crime has been committed or imminent and a search is refined for evidence-gathering, the crime committed must be a common law crime or criminal misdemeanor and allegation has been made against a particular person.

The Crimes Act 1914 sets out that in order to obtain a search warrant the investigator must denote that there are reasonable grounds for suspecting there are evidential materials on the location by a search warrant and depict adequate evidence that the

person whose location is targeted by search warrant is in possession of evidential material. The investigator should also state the crime relating to the search warrant, describe the location, the evidential materials to be searched for and the time the warrant of search will be executed. The researcher's experience is that, in the case of computer-related crime, the investigator must ascertain the role of the computer in the alleged crime and chronicle facts depicting how intangible evidentiary materials are associated to the crime location. This can be achieved by using Internet Service Provider (ISP) in establishing connection between items listed in the search warrant and the location to be searched using Internet Protocol (IP) address.

Kerr (2005:103) argues that computer-related crime, because of its nature, gives a challenge in establishing connection between location to be searched and listed items because it has no physical boundaries. United States Department of Justice Search and Seizure Manual (2002:179), however, expresses a variance between static IP address and dynamic IP address such as Dial-up connection which provides a temporary IP address each time it connects to the internet and is discontinued if there is no longer connection to the internet and the address assigned to a new user. This makes the location of the suspect impossible to track although a probable cause can be established if they remain online. According to the United States Department of Justice Search and Seizure Manual (2002:179), a static IP address is unique and permanently assigned to a computer connected to internet in a fixed location. Although they lead to the names and physical locations of the subscribers, there is a challenge in connecting to the location to be searched because suspects can access other devices associated with static IP address. Nevertheless, in several scenarios, there will be a problem in establishing a nexus between the static IP address and the physical location to be searched. This makes the probable cause to search every computer invalid. (United States Department of Justice Search and Seizure Manual, 2002:180). There is no case law in Zimbabwe that addresses the issue of IP address and probable cause, although searches are based on reasonable grounds that a search will expose evidence regardless of whether the belief is correct or not.

The researcher's opinion is that, the reasonable grounds threshold used to justify issue of a conventional search warrant must be used to obtain computer-related crime search warrant. In the Zimbabwean scenario factual evidence connecting the crime, the items to be searched for, the location of the search is crucial in preparing the search warrant. (Feltoe, 2009:20). The search warrants have actually been used to search for tangible things whereas in computer-related crime data is the instrumentality of crime and the search is for intangible items, such as data, images and files.

According to Mukuruba (2013), in matter of S v Mutemi 1998 (2) ZLR 290 (HC), the court held that the general principle of Roman-Dutch law that intangible things are incapable of being stolen have no place in the digital world and exceptions have emerged against the general statement of law. In the case of S v Ndebele and another (SS16/2010) [2011] ZAGPJHC 41; 2012 (1) SACR 245 (GSJ) in addressing the question of 'whether or not electricity can be stolen, it was held that such intangible things could be stolen. The researcher is, however, of the opinion that the procedures outlined in the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 relating to search and seizure in Zimbabwe is insufficient to address searches related to digital context although in the foregoing judicial precedence the definition of property now includes digital items. Search Warrants must distinguish the scope of the search, meaning the investigators should search only for materials that are depicted in the search warrant and authorised by such search warrant. In the case of Elliot v. Commissioner of Police 1986 (1) ZLR 228 (H) it was held that the search was rendered invalid because it was too general and vague. The court ordered return of evidence that was not listed in the search warrant.

Computer-related crime search warrant deals with two different categories of evidence, thus the hardware and software as these two require different searching tactics although they are interrelated. The challenges emerge in a complicated network like Local Area Network (LAN) where several computers are connected to it. Kerr (2005:104) stresses, searching and seizing network, its infrastructure and computers and its peripherals can

be achieved through a search warrant. This may, however, create business disruptions and invasion of privacy of people not connected to the crime. Welty (2011:7) suggests search warrants have a principle of specificity which means, they can only be issued for a defined crime, location and list of items to be searched for and seized. However, this approach poses a challenge because in the process of searching incriminating data may emerge blended with other files where extraction of evidence cannot be done on site. The scope of the search will likely proceed beyond the principle of specificity, particularly where a search warrant excludes other documents subject of the search and out of ignorance that they do exist. In some instances this has been substituted by mirror copy searches. Law Commission Report (2007:198) says this is, however, an exception where the whole business is to be searched on the belief that all the computers nurse evidence and unrestricted search will be valid.

Brenner and Frederiksen (2002:99) argue that at times digital evidence is harboured by professionals and skilled personnel who are able to conceal evidence and specificity will incur additional time and costs. Therefore, the mirror copy search is significant for retrieving relevant data although the current procedure in Zimbabwe does not deal with computer-related crime searches and mirror copies. This leaves conventional search warrant applicable to computer-related crime searches. The Fourth Amendment and the Privacy Protection Act (PPA) of 1980 protects individuals from arbitrary broad search and seizure. However, by virtue computer related crime is different from traditional crimes as it involves use of forensic tools to extract evidence. The Sixth Circuit in Guest v. Leis, 255 F. 3d 325 - Court of Appeals, 6th Circuit 2001 ruled that the incidental search of PPA protected material blended in the suspect's computer with evidence of a crime does not give rise to PPA liability as it requires the owner's cooperation to split materials. The foregoing approach will be permissible under the Zimbabwe Criminal Procedure and evidence Act 14 of 2004 where there is no feasibility of precisely describing the location because the suspect has provided hurdles and items to be searched are voluminous.

3.4.1 Off-site search

According to Jarrett and Bailie (2009:77), searching a computer on-site is generally observing the screen to establish information relevant to the search warrant at hand. However, it may proceed to opening of files and printing of documents. This is because some evidence will be held in the computer's RAM which tends to offer a temporary and volatile storage. If computers are switched off data located in the RAM will be erased or altered. Brenner and Frederiksen (2002:46) point out that off-site search occurs when investigators retrieve computers, documents, files, and programmes, to an off-site location for a search. This is done because digital evidence recovery and applicable logistics cannot be achieved on-site. Welty (2009:9) argues that computer-related crime should not be conducted off-site since investigators can use electronic searching techniques to achieve fast and accurate searches on site. There is also a concern that off-site searches tend to cripple businesses and unnecessary interruption during the course of the investigation. Brenner and Frederiksen (2002:46) reiterate and say if the computer to be searched is a stand-alone with a small storage capacity, the off-site search will be unreasonable, because current forensic tools are able to locate the evidence in real-time.

Jarrett and Bailie (2009:80) argue with what Welty (2009:9) is asserting *supra* and say searching files on-site has its own risks such as damaging the evidence related to uncommon operating systems and that off-site searches are necessary as some of the computers are "booby trapped" by savvy criminals. On-site skilled users may use trip-wires with self-destruct programs to delete evidence (United States Department of Justice Search and Seizure Manual, 2002:179). There is also some considerable time required to search files at the scene and that can extend to several hours or even days (United States Department of Justice Search and Seizure Manual 2002:180).

Brenner and Frederiksen (2002:54-56) mention five issues that should justify off-site search and these are;

- Whether other options are applicable in the presented location.

- Whether there are options to access evidence without resorting to off-site equipment or expertise;
- The probability of damaging or destroying evidence if an on-site examination is done.
- Whether there is need to use off-site equipment or expertise search and preserve evidence.
- The duration of time required to search for evidence on-site

Jarrett and Bailie (2009:76) in their discussion say it will be ideal if a flexible approach of off-site search is permitted as the computer related crime makes on-site search impractical and does not give the investigators a leeway on what and where to search although this can be substituted by mirror copy search.

3.4.2 Search without a warrant

According to Feltoe (2009:20), laws are provided to ensure that individual privacy prevails whilst investigation and entry to collect evidence is not hindered. International Human Rights Law, for example, recognises that individual privacy rights are not absolute and must be balanced with a government's interest in detecting and combating crimes. There is, however, exceptional in circumstances where obtaining a search warrant is very difficult or impracticable and the investigators are empowered to search and seize evidence without an official search warrant. The Zimbabwe Criminal Procedure and Evidence Act, deals with conventional legal concepts of warrantless searches and seizures. The exceptions to search without warrants are: exigent circumstances, consent searches, plain view searches, and searches to do a lawful arrest. Section 51 (1) of the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 provides that a search and seizure can be done without a search warrant if the person concerned consents to the search for any additional articles or, if the investigator on reasonable grounds believes that a warrant would be issued to him and the delay in obtaining a warrant would prevent the seizure or defeat the object of the search. In the Chizano v. Commissioner of Police HH-392-88; Associated Newspapers of Zimbabwe (Pvt) Ltd v Madzingo NO & Anor HH-

157-03 case the court ruled that; before the police may lawfully search without warrant and seize items during that search two conditions must be satisfied, namely;

- “the police officer seizing the items must believe on reasonable grounds that a warrant would be issued to him by the appropriate authority if he applied for one; and;
- he must believe, on reasonable grounds, that delay in obtaining a warrant would prevent the seizure”.

Section 53 (a) (b) of the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 authorises any person lawfully in charge or occupation of any land and who reasonably suspects that , stolen stock or produce is upon or in any premises on that land or any article has been placed upon or in any premises on that land or is in the possession or under the control of any person upon such premises in contravention of any law relating to harmful liquids, dependence-producing drugs, arms and ammunition or explosives; may at any time, if a police officer is not readily available, enter the premises for the purpose of searching the premises and any person thereupon or inside there and, if stock, produce or article is found, he shall take possession of what is found and deliver it to a police officer. This is, however, silent on the digital evidence context. Other government departments have the powers to perform searches which are relevant to accomplish their tasks without a search warrant, for example, the Zimbabwe Revenue Authority (ZIMRA) in examining luggage of travelers and Health Inspectors in examining supermarkets and butcheries.

Section 52 of the Zimbabwe Criminal Procedure and Evidence Act 14 of 2004 states that if a state investigator has reason to suspect that an offence has been committed by any person on board a boat on inland waters, it shall be lawful for him to stop, go on board and search such boat without warrant and to seize anything which he has reasonable grounds for believing will afford evidence as to the commission of an offence under any law. This is applicable to conventional searches and in the absence of any procedures related to digital evidence; the warrantless concept is also applied to computer-related crime. Section 52 (1) of the Zimbabwe Criminal Procedure and Evidence Act 14 of 2004 asserts that on the arrest of any person the State investigator may search any person

and seize any article which is in the possession or under the control of the person arrested.

Section 52 (2) provides that any State investigator may stop and interrogate any person who is found at any time between sunset and sunrise carrying or transporting any goods or articles of any description and if (a) such person does not account satisfactorily for the possession of the goods or articles so being carried or transported; or (b) there are reasonable grounds for suspecting that such goods or articles have been criminally procured. Whilst these pieces of legislation may apply to searching of computers they may cause a problem if the searching progresses to off-site searches. The Zimbabwe Criminal Procedure and Evidence Act 14 of 2004 exclude provisions related to searches of digital evidence and Investigators are guided by the laws relevant to warrantless searches of traditional objects.

3.4.3 Scope of consent

According to 51(1) (a) (b) of the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004, a police officer may, without warrant, search any premises for the purposes of seizing any article if the person concerned consents to the search. The search and seizure of the article in question can also be done without consent of the person concerned, if he has reasonable grounds that, a warrant would be issued should he apply for it and that, the delay in obtaining a warrant would defeat the object of the search. United States Department of Justice Search and Seizure Manual (2002:10),posits, “consent:” means willingly agreeing to make an intelligent choice to approve something proposed by another to a person in the possession of and who exercises sufficient mentality. The essential elements to consent are viewed as free choice, ability to make a decision and communication between persons. The foregoing suggests consent must be informed and the consenting party serves a right to refuse to give consent. Section 51(1) (a) of the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 says consent is an exception to the search warrant requirements and should be approved by a person

with authority to approve the search. Consent should therefore be based on the following to determine its validity:

- Whether the consent is express or implied,
- Whether the scope of the consent is limited or unlimited, meaning investigators should confine their search to the places delineated by the consent.
- Whether the consent is obtained before or after the search,
- The status of the person who grants the consent.

United States Department of Justice Search and Seizure Manual (2002:11) states in the USA, the courts determine the validity of consent through the age of the consenting party and the person's level of education, intellectual strength and mental condition because these aid in determining if the consenting party is able to distinguish between physical and digital searches and the risk linked to digital searches. There is also need to determine the physical condition of the consenting party, whether the person was under arrest and that the consenting party was made aware of his rights to refuse consent.

In the Zimbabwean setup investigators are able to obtain consent to search computers and digital evidence, although, the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 does not provide that consent should be written or recorded. In digital evidence the consent could be validated by disclosure of passwords by the consenting party. Sady (2012:20) mentions that the scope of consent is portrayed in two scenarios, firstly, the extension of physical search to search digital devices and secondly, the digital search of other devices or files not specified in the initial consent. Jarrett and Bailie (2009:16) indicate that, to eliminate invalidation of consent, the investigating officer must present a written consent form depicting the scope of consent by including information on the search location, what the investigator wants to achieve with the search and his desire to search within any computer or technological device found within the area.

Brooks (2004:4) suggests that the consenting party should have control of the computer including the data contained therein and any area in the device in which the consenting party is allowed access. Therefore, consent should cover the whole contents of the computer.

According to United States Department of Justice Search and Seizure Manual (2002:12), third party consent is a relatively new exception which requires individuals other than the householder to consent to a search of shared location without a warrant. In computer-related crime, third party consent is favourable to devices such as computers, networks and internet that are shared amongst multiple users. The third party consent doctrine is also relevant in work places where employers may consent to searches and seizure of evidence from their employees. United States Department of Justice Search and Seizure Manual (2002:13) mentions that third party consent in computer-related crime is in the form of local; thus geographical proximity and remote consents which are unique and only relevant to digital searches. Internet and networks make the remote search practicable. The administrator of the network can give third party consent.

3.4.4 The plain view doctrine

In Zimbabwe, the plain view doctrine is applicable in terms of s 26 of the Serious Offences (Confiscation of Profits) Act [*Chapter 9:17*] which says, a magistrate may issue a warrant to search for "tainted property", which includes property used in connection with serious offences and the proceeds of serious offences committed inside and outside Zimbabwe, although the kind of property to be seized must be specified in the warrant, the police nonetheless may seize property which they believe on reasonable grounds to be, tainted property in relation to the offence even if it is not specified in the warrant, tainted property in relation to another offence and, anything believed on reasonable grounds to be able to afford evidence of the commission of ‘a criminal offence’. The Zimbabwe Criminal procedure and Evidence Act, 14 of 2004 authorises officers to seize evidence not described in a warrant and presenting itself in plain view of investigating officers

According to Sady (2012:25), the plain view doctrine is a legal concept deduced from three landmark decisions, Coolidge v. New Hampshire (1971), Arizona v. Hicks (1987), and Horton v. California (1990). Jarrett and Bailie (2009:34) conclude the plain view means evidence in plain view of the investigator who has a right to search may be seized.

Kerr (2005:567) states plain view means “unpredictably locating evidence, without possessing prior knowledge that such evidence existed in that location and without executing any physical search to find it.” Plain view concept occurs during execution of a search warrant when evidence not mentioned in the search warrant surfaces and is seized. Brooks (2004:1) asserts that there is a challenge with plain view doctrine in relation to computer-related crime. This is because the documents, files and databases stored in computers are intermingled and are either latent or active. Whilst forensic tools are capable to retrieve hidden or deleted data, the plain view doctrine applies to visual observation without a search.

Kerr (2005:577) advanced three methods which might limit the applicability of plain view doctrine in computer searches and posits that forensic tools diminish the plain view doctrine, plain view doctrine will be accepted where the crime is serious and that annihilation of the plain view doctrine in computer crime-related searches poses challenges when applied in digital environment. On the other hand, United States Department of Justice Search and Seizure Manual (2002:20) argues that, the plain view doctrine may be applicable in digital searches if the following are adhered to:

- The source of evidence should be accessed legally by including in the search warrant the nature of electronic storage and the desire to examine the entire contents of the device.
- The apparent illegal nature of the evidence is immediately known, for example, in the investigation of a Disk Operating System (DoS) attack; the investigator can seize pornography images displayed on the computer’s screen.
- The investigator should not abandon the original search.

Brooks (2004:7) further highlights that, in computer searches, whether it is not immediately clear that evidence retrieved falls within the scope of the search warrant, the investigating officer has to carry out further examination to establish that.

3.5 APPLICATION OF TRADITIONAL SEARCHING PROCEDURES OF PHYSICAL OBJECTS TO INTANGIBLE OBJECTS

The Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 providing for search with or without a warrant does not avail clear guidance for conducting computer searches. Therefore, the existing law does not clarify the distinction between tangible and intangible so as to explicitly define unique aspects of searching intangible data. For example, investigators conducting a lawful search are often unaware whether material is held in tangible or intangible form. Therefore, any application for a separate search warrant on finding devices storing evidential material would be more restrictive than for tangible material. Cassim (2009:67) mentions that there is need to review search procedures to include intangible evidence derived from computer-related crime as well as the issue of jurisdiction is influenced by technical characteristics of the Internet.

The researcher asked the participants if according to their knowledge, traditional searching procedures applicable to physical objects were also applicable to the intangible objects. Thirty participants from sample A and three participants from sample B said the existing searching procedures of physical objects under the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 were also applicable to intangible objects. The eleven out of thirty six dockets in which searches were done show that only physical objects were recovered; however, the procedures were not explicitly depicted.

According to the European Convention on cybercrime (2001:111), traditional search laws apply to tangible physical objects; this is because data is intangible and can only be read with the aid of computer equipment or software developed for such purposes. European Convention on cybercrime (2001:112) further argues that traditional search laws may enable the search of computer systems but have legal limitations if the search is to be extended to computer data storage mediums. United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000:8) in agreement with European Convention on cybercrime (2001:111) indicate that traditional searching procedures provide for searching of the entire computer system as it does with any other physical objects. The researcher notes that the investigator's powers are diminished when the

contents of computer have to be investigated against the will of the owners and this is further compounded in a multi user environment.

United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000:8) and Cassim (2009:67) stress that the investigator using traditional powers to secure data may face challenges related to access to the computer system, the intangible nature of data and data may be stored in another connected system located away from the premises being searched. United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000:8) mentions that in traditional searching procedures tangible objects are searched and secured in their physical state whereas in data copies are made. According to New Jersey Computer Evidence Search & Seizure Manual (2000:11), tangible objects are tangible computer equipment that occupy physical space and their location is clearly described for search purposes. New Jersey Computer Evidence Search & Seizure Manual (2000:11), further posit that intangible objects are mainly computer data in a computer which may be connected to other computers and servers providing for divers physical locations. Information sought by the search may not only be at the location but at a remote location as well and accessible to anyone sharing that network.

The researcher is of the view that the prevailing practices will be ideal to gather intelligence before applying for a search warrant, particularly on the computer equipment at the search site and its network. On the hand, during the process of gathering such intelligence, suspects may be alerted leading to destruction or alteration of evidence.

3.6 BASIC STRATEGIES AND PROCEDURES FOR SEARCHING COMPUTER EVIDENCE

Zimbabwe does not have a legislative enactment or manual that prescribes the strategies and procedures for searching computer evidence. Section 50 (1) of the Criminal Procedure and Evidence Act, 14 0f 2004 provides that the Zimbabwe Republic Police are the only authority empowered to execute search warrant. In regard to the pre-digital stage, whilst the suspect may not be notified of the search, their presence during the

search is sought for and handed over a copy of the search warrant or another person present at the premises. They may as well elect to have their lawyer present. In the digital phase there are no relevant provisions in the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 that can be applied in computer searches and seizures. Whilst the investigator ensures the details of the search are contained in the search warrant, he will identify himself and have the power to gain entry into premises without prior warning.

According to Farmer and Celentano (2000:3), prior to searching there is need to identify the targets of crime, the computer systems to be searched and software, hardware and networks employed by the targets. Welch (2012:2) illustrates that there should be an incident response plan that includes formulation of a team. Judish (2002:42) suggests that the team should include investigating officer and computer forensic experts. Judish (2002:42) concurs with Robbins (1994:8) that the team should also be responsible for the preparation of the warrants, items to be listed in the warrants and consideration of exigent circumstances. Reith, et al. (2002:2) and Ami-Narh and Williams (2008:2) all affirm the importance of the foregoing strategy and further state that the team will have to learn and recognize the incident and the systems that will be searched so that they prepare the tools, techniques and summon management support.

According to Kerr (2005:92-93), in traditional searching, the objective is achieved in three stages. Firstly, knocking and notifying the occupants followed by selecting the appropriate pattern of search. The second stage is rummaging and opening of items; and the third and final stage is the seizure of what has been obtained from searching.
Trepel (2007:122) points out that, in computer-related crime, the search warrant execution refers to data processing through forensic analysis and it is in two stages:

- The pre-digital search on-site and it mimics the first stage of the traditional search procedures, such as notifying and observation of location to be searched. It also includes applying searching tactics and identification of digital devices, documentation, recording and video shoots. This is followed by labeling all the cables as this will aid in the reconnection on reassembling the device. There is

also power management of RAM and system used such as Windows XP, Linux, UNIX, and Macintosh, as each of these systems uses a different mechanism for storing and running files stored in RAM. In some systems the data in RAM is lost instantly upon switching off of power.

- The digital search works with data and is normally conducted off-site at divers' times and by different forensic officers. It is done in order to determine invisible and intangible evidence from the hardware devices that were preserved in the pre-digital stage. Evidence attained at this stage may contain history files and the object of the crime.

According to Shipley and Reeve (2006:3), these stages negatively encroach into each other's way. For example, application of pre-digital search procedures may result in evidence being destroyed or contaminated. In order to avoid the foregoing evidence must be secured both physically and digitally. Welch (2012:2) emphasizes that the physical can be achieved by barring access to the computer whether physically or any other connection including over the network. This is achieved by removing phones from the saddle or unhooking them, identifying booby traps and isolating computers from network connections. The researcher's experience is that in cases where there is more than one computer, it will be ideal to first secure the one in the suspect work desk or room. The crime being investigated will give guidance to where the digital in question is lodged although there is need to summon the help of experts to examine the media at hand whilst ensuring there is no wire interference during the examination of the scene. The wireless network connections are capable of deleting files and programmes remotely.

In the USA, section 213 of the Patriot Act of 2001 authorises the person executing the search to apply a "sneak and peek "search, thus to secretly enter into premises physically or electronically to carry out a search. The Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 does not subscribe to such provisions, although this is viewed as the best way of overcoming the weakness in the pre-stage procedures. Thirty participants from sample A and three participants from sample B when asked of the basic strategies and

procedures for searching computer evidence professed ignorance and were not comfortable in answering the question. The eleven out of thirty six dockets where searches were done do not depict any strategy employed to pursue the searching procedure of computer evidence. This affirms the response given by the participants in this area.

The researcher's views following assertions by the foregoing authors are that the traditional procedures of knocking and notifying negatively affects the integrity of the evidence retrieved as it may have been tempered with. It will be ideal to surprise the suspect and this gives the sneak and peek search an edge over other procedures. The requirement of the Zimbabwe Criminal Procure and evidence Act, 14 of 2004 of handing over a copy of the search warrant puts the suspect at an advantage. It provides the suspect an opportunity to tap on a device and evidence is interfered with unless there are reasonable grounds to gain entry without announcement.

Reith, et al. (2002:2), Ami-Narh and Williams (2008:2) and Judish (2002:42) agree that both pre-digital and digital stages require both conventional and digital tools to accomplish search strategies and objectives. The first strategy is deploying the first group to secure the physical location and the second group consisting of investigators equipped with knowledge to perform both computer-related crime and traditional searches. The latter group will handle the physical issues, suspects, technical equipment and other investigations. Shipley and Reeve (2006:4) state that the investigators must strategize not to change evidence during the search of a running computer. Shipley and Reeve (2006:5) defined a running computer as a computer powered on upon encountering at the computer- related crime scene. Shipley and Reeves (2006:5) further highlight the listed steps will enhance strategies for searching computer evidence and will not have any effect on the overall state of the evidence:

- A log must be maintained on all actions on running machine during the search.
- The screen on the running system should be photographed and Wilkinson (2010:8) suggest in the absence of a camera a sketch plan should be drawn.

- The running machine's operating system must be identified.
- The actual time must be recorded against the date and time on the screen of the system being searched.
- The RAM should be dumped from the system being searched to a removable storage device.
- The system must be checked for the use of the whole disk or file encryption.
- There is need to determine how searched evidence will be seized
- All steps taken during the search must be documented.

According to Farmer and Celentano (2000:55), the strategies and procedures for searching of computer-related evidence include the following;

- Shutting down the computer system by removing its plug from the electrical outlet or using applicable commands to shut down a network computer. There should be a consideration for any operations running in the back ground such as memory or modem.
- An appropriate chain of custody should be activated by creating evidence tags during the search whilst taking pictures of the computer from numerous angles to document the system peripherals and their connections before the computer is actually dismantled. Each wire should be labelled to easily reconnect after the system configuration has been reinstated.
- During the search the computer should not be run and evidence should not be processed until bit stream backups have been made of all hard disk drives and floppy disks.
- During searching, the system date and time should be recorded.
- The forensic investigator may use search tools to uncover relevant evidence based on information collected on key words to search the entire computer hard disk and any floppy disks.
- During the search the swap file should be examined because in some operations such as Windows 95 or 98 it is created by default and it is erased when the computer is turned off.

According to the Scientific Working Group on Digital Evidence Version (2006:3-4), before any searching is done the legal authority to search must be reviewed and obtain additional authority for any evidence outside the scope of the search. Scientific Working Group on Digital Evidence Version (2006:3-4) stresses that if the computer is off it should not be turned on and before powering down a computer ensure the encrypted data is captured. In cases of networked computers it will be ideal to remove the power connector from the computer's back and apply evidence tape on the plug connector on the computer's back. On servers appropriate commands should be used to shut down. Thomas and Forcht (2004), however, seek to differ and state more experts recommend pulling the plug off even if the computer is running. The benefits are that any script about to be executed upon shutdown does not get a chance to run and temporary word processing and other interim files remain on the hard drive whereas they could be deleted if the software application shutdown is done more gracefully. Wilkinson (2010:8) tends to differ in that if power is removed from running system any evidence stored in encrypted volumes will be lost, unless relevant key is obtained.

3.7 ACCEPTABILITY OF EVIDENCE RETRIEVED THROUGH SOFTWARE TOOL DURING TRIAL

In the matter of S v Bennet (CRB 178/09) 2010. ZWHHC 79, the defence successfully claimed that, the laptop which was confiscated from Michael Hitschmann was tempered with, when it was moved from the exhibit office to the office of the police officer commanding province. The state could not explain, how the emails in the laptop were downloaded. The witness perceived to be an expert could not explain the software used to extract emails. According to Forensic Examination of Digital Evidence, A guide for law Evidence (2004: 3), the software used to search for evidence should be appropriately licensed otherwise its use will be successfully challenged in court. This is reiterated by Schatz (2007:29) that software licensing has been proposed as a solution to reliability of tools supporting searching of digital evidence. John (2012) posits in pursuit of searching practices of digital evidence, the British Standards Institution (BSI) for legal admissibility and evidential value of searched digital information prepared a series of codes of practice.

John (2012) further states that in the US, the Scientific Working Group for Digital Evidence (SWDGE) sets up standards for searching, preservation and examination of digital evidence and the Digital Evidence Group (DEG) in the United Kingdom (UK) has a similar function. When asked of the acceptability of evidence retrieved through software tools during trial, ten participants from sample A indicated that expert evidence regarding computer related crimes extracted through software tools is accepted because there is no any other evidence to rebut it. Eight participants from sample A posited that, for a proper decision in court the presiding must be knowledgeable in diverse software tools, information and technology. Twelve participants from sample A said the majority of judges tend to afford the evidence extracted through software tools unwarranted presumption of reliability. Three participants on sample B indicated that, there is need for technical knowledge before accepting and interpreting computer related evidence extracted through software tools. The thirty six dockets perused do not show that software tools were ever used in retrieving evidence.

According to John (2012), a number of court cases have emphasized on the requirement for scientific procedure and methodologies used to process the procedures. John (2012) and Ryan and Shpantzer (2008) citing the case of Frye and Daubert in the USA, *Frye v. United States,* 54 App. D.C. 46, 47, 293 F. 1013, 1014(1923), in which the courts set precedence that where the community accepts a scientific procedure the court will adhere to this general acceptance. John (2012) and Ryan and Shpantzer (2008) further state that the foregoing precedence was upheld in the matter of Daubert vs. Merrell Dow Pharmaceuticals, (92-102), 509 U.S. 579 (1993) and besides general acceptance there should be testability, peer review, known error rates and existing standards. According to Marsico (2005:9), tools used for searching evidence should be tested for accuracy and uniformity so that evidence searched for will be proven and reliable. In computer forensics hardware tools consisting of devices that interface with computers are tested for their operability. Carrier (2002) as quoted by Marsico (2005:9) presents two scenarios related to testing of software as:

- Open source testing; the investigator and the courts trust that the software application was created, coded accurately and properly for reliable results.
- Closed source testing; is done by the public although the vendor retains the code.

Schatz (2007:29) mentions that in evaluating the two foregoing scenarios by Marsico (2005:9) it is apparent that in the open source testing there is excessive reliability placed on the producer of the software. On the hand, the availability of access to software codes aids the software integrity verification process. According to Marsico (2005:10) and John (2012), the National Instate of Standards and Technology (NIST) through the United States (US) Department of Commerce established a team, namely Computer Forensic Tool Testing (CFTT) that is working on definition requirements for disk imaging tools. Kent, et al. (2006:4-7) corroborate that this is to ensure investigators can depend on tools that are tested although it is limited to tools that copy or image hard disk drives.

John (2012) concurs with Marsico (2005:11) and Ryan and Shpantzer (2008) that, as a requirement for admissibility, there is need for the tools to be subjected to peer-review and error rates:

- Peer review; that is exposing the tools to both the public and expert scrutiny before considered admissible. This creates peer collaboration, open research, retesting coupled with divers' analysis. The challenge is that the experts expected to review the systems are not well defined in computer forensics.
- Error rates; the test is done both on tools used to search for evidence and the methodologies used to determine the known error rates of the relevant tools used to search for evidence and the potential error rates of methods used.

The foregoing will aid the courts in making decision on admissibility of evidence collected using the tools and methods. Thomas and Forcht (2004:696) agree on the foregoing with Marsico (2005:11) and *cite* the precedence in the 1993 US matter of Daubert vs. Merrell Dow pharmaceuticals (92-102) 509 U.S. 573 (1993) that set out five elements. The five elements provide the acceptability of evidence gathered through unproven techniques or methods consisting of the probability of testing the theory or technique. They also provide the intervention of peers and probably publication, the known or potential error, the

acceptance by the community in the scientific fraternity and the testimony based on the expert's unique skill. Sherman (2006) illustrates the five elements depicted by Thomas and Forcht (2004:696) and Marsico (2005:11) are fundamental to convincing the courts of the reliability of the software used in searching for evidence. Anti-cartel enforcement manual (2010:26) supports this by stating it is good practice that tools used are tested and accepted in computer forensics. FBI Law Enforcement Bulletin (2011), in another dimension mentions that for electronic evidence to be accepted requires tools to be calibrated with records to that effect retained as evidence to sustain the accuracy of the tools.

3.8 THE IMPORTANCE OF CHAIN OF CUSTODY WHEN COLLECTING AND PRESERVING COMPUTER CRIME EVIDENCE

According to Madhuku (2010:10), "chain of custody" is the strict handling is required for all electronic evidence seizures to avoid compromising of the potential evidence. A register should be maintained to provide direct evidence of unbroken chain of possession of seized evidence up to its disposal. Ryder (2002:2), says, a chain of custody is the process of preserving the integrity of the digital evidence by ensuring that it is not broken. Witter (2001), mentions, a chain of custody is a guideline that demonstrates the method used to search and collect evidence, analyse it, and preserve it in order to present it in court. Chval (2006:39) states that "the chain of custody is the device that the proponent of an item of evidence uses to authenticate that an object is what it purports to be." According to Nandhakumar, Agarwal and Faizal (2012:50), chain of custody is the procedure used to conserve and document the sequential history of evidence. Gayed, Luonis and Bari (2012) proffer a definition almost with similar essential elements to Nandhakumar et al. (2012:49) adding that a chain of custody document is used to substantiate the guideline of how evidences have been copied, transported, and stored in the entire investigation process.

The participants were asked of the importance of chain of custody when collecting and preserving computer crime evidence and twelve participants from sample A suggested that chain of custody is important as it identifies changes in the control, handling,

possession, ownership and custody of piece of evidence. It also entails audit trail of the route that the evidence took from the time it is collected until it is presented in court. Eleven participants from sample A indicated that chain of custody reduces the chances of evidence contamination and tempering. It accounts for all persons who handled or who had access to the evidence in question. Seven participants from sample A pointed out that it provides for protection and accountability of evidence. Three participants from sample B highlighted that it acts as means of accountability that shows who obtained evidence, where and when, who secured it, who had control and possession of it. The researcher agrees with all the participants that chain of custody protects the integrity of the evidence and its effective process of documenting the complete journey of evidence during the life of the case. All the thirty six dockets perused indicate that the chain of custody is well maintained on the running diary logs, crime report forms and exhibits are well labelled with the unique numbers reflected on the forms that also provide for chain of custody signatures.

In view of the foregoing definitions, Nandhakumar et al. (2012:51) contend appropriate methods have to be devised to sustain a standard way of capturing all details, commencing with first, the scene and all other persons who have custody of evidence. The details should also consist of date, time, user authentication, file name, case number, brief description of evidence and storage location (Chval, 2006:39). Gayed, et al. (2012) support Chval (2006:40) by stating that the following questions should be asked to prove that evidence has not been altered in the entire process;

- Who searched for digital evidence including those who came into contact and handled it?
- What were the procedures used to search and discover evidence and what was done to it and who obtained it?
- When was the digital evidence discovered, accessed, examined, or transferred?
- Where digital evidence was discovered, collected, handled, stored, and examined and who secured the evidence and who had control or possession of the evidence?

- Why the evidence was collected?
- How was the digital evidence searched, collected, used, and stored?

Ryder (2002:5) emphasizes that this process is applicable to both the physical hardware and information searched and retrieved from that hardware. Nandhakumar et al. (2012:49) further state documenting chain of custody will ensure collected evidence is authenticated, valid and integrity is sustained by ensuring that handlers do not tamper or destroy evidence. Daley (2010:63) mentions that, to ensure chain of custody is maintained, the physical integrity of the computers and media should be sustained by tagging each item and matching it to the persons who searched, preserved and transported data. Information Security and Forensics Society (ISFS) (2004:13) acknowledges that this process continues through process of the trial until the evidence is returned to where it was collected from. Witter (2001) and ISFS (2004:13) further state that preservation of chain of custody can be achieved by ensuring that there is no addition or alteration of information and the copy made was complete. It can also be attained by ensuring that copy process used was reliable and entirety media was secured to ensure original copies are sustained.

Witter (2001) in citing United States US Code Title 28, Section 1732 notes chain of custody log files are admissible as evidence only if collected during the course of normal business and there is proof that they have not been tempered with. This can be achieved by using digital signatures to verify log authenticity and these should be maintained throughout all processes. According to ISFS (2004:13) it is critical to ensure that reliable copy process was used by testing if the process is compatible to prevailing industry standards, if independent verification of copies can be achieved and whether the copies were subjected to tamper proof.

Dykstra and Sherman (2012:3) in their discussion mention that in computer related evidence there should be chain of custody for both physical evidence, for example, the computer and its peripherals and; data contained therein, for example, copies of data like

MD5 checksums need careful handling. Dykstra and Sherman (2012:7) assert that transfers of custodianship of such evidence must be documented by a digital derived system. Dykstra and Sherman (2012:2) reiterate Ryder (2002:2) by mentioning that data need to be copied on media such as CD-ROM using consistent methods and all processes adopted to search and capture the data, including changes made, well documented.

Newby, Schwarz and Carroll (2005:46), Ryder (2002:2) and Dykstra and Sherman (2012:4) concur that once a forensic image of the original data is created and copied to a hard disk drive there should be chain of custody and running logs for any access to the hard drive image. According to Garfinkel (2009:1), accurate logs relating to digital evidences must be audited. Newby et al. (2005:47) suggest that hash validation is a reliable authentication to prove that an image is an exact duplication of the original, particularly where there is chain of custody depicting the time the computer was seized and the image created. Chval (2006:40) claims the best ways of ensuring chain of custody in computer-related crime is by being pro-active and design a plan that entails the following:

- The procedure of searching a computer to ensure that files are not negligently altered.
- All the devices and peripherals must be documented before they are searched and a digital camera will be relevant in such circumstances.
- On collection all items to be marked with a unique number.
- The date, time, personnel and purpose for every transfer of custody is recorded.
- Avail storage with suitable condition and ensure there is no alteration or destruction of digital evidence.
- Avail evidence that validates the forensic tools did not create alterations to data.
- Create Hash values of files or media by running a sophisticated algorithm against a set of data, such as file, CD or hard drive.

Chval (2006:39) and Gayed et al. (2012) mention that digital evidence is inclined to easy alteration and it will be ideal to provide a witness to testify that the data is the same condition when it was searched for and seized and the absence of missing links.

Giova (2011:1) argues that in view of software used to acquire copies or images from electronic devices, the chain of custody of software and data cannot guarantee the quality of forensic images and that an appropriate person accessed evidence through authorised manipulation. Therefore, according to Chval (2006:40), digital evidence is considered as valid if the chain of custody can demonstrate where, when and who came into contact with electronic evidence in each stage during the investigation. Garfinkel (2009:2) mentions that traditional chain of custody consists of creating and updating paper or electronic forms with information related to particulars of investigators, description and hash codes. However, modern forensic software provides enhanced evidence description, electronic user identification, automated audit trail and digital signatures. Garfinkel (2009:4) further adds that authentic digital signatures are critical in establishing chain-of-custody because they consist of non-repudiation properties.

3.9 USE OF COMPUTER FORENSIC EXPERT TO SEARCH AND PRESERVE COMPUTER EVIDENCE

According to Bui et al. (2003:22), the expert has comprehensive techniques and knowledge of formats in which evidence can be searched. Bui et al. (2003:32) further states that an expert has capabilities of making the necessary backups without eliminating or tampering with evidence. Meyers (2005:15) adds in court, opinion of an expert witness is admissible as evidence in cases where lay persons are incapable of presenting correct judgment upon the matter that requires scientific knowledge, a previous habit or experience or study. In corroborating the foregoing, Meyers (2005:36) *cites* the matter of *Frye v. United States,* 54 App. D.C. 46, 47, 293 F. 1013, 1014(1923). Meyers (2005:46) further asserts that, in computer-related crime, experts should be used for examination, analysis, interpretation of evidence because of their theoretical and practical knowledge of emerging tools, technologies and legal changes. Crouch (2010) in his discussion mentions that this is because computer forensic experts have capabilities to gather and document evidence step by step, not only from the original device, but on a replicated

digital image of the original thereby eliminating legal assumptions that evidence was altered during the search. Dougherty (2002) reiterates computer forensics expert possess a wide variety of skills in which in some instances is capable of developing their own suite of software forensic tools and sustain admissible chain of custody according to legal requirements.

On asking the thirty participants from sample A and three participants from sample B on the use of computer forensic expert to search and preserve computer evidence, all participants indicated that they have never used any experts in the investigation of computer-related crime matters as these experts were not readily available to assist them in their investigations. On the thirty six dockets perused there were no experts used to search for computer-related evidence. According to Meyers (2005:46), in the United States, to ensure quality of expert evidence is sustained, the expert court testimony is reviewed annually for quality control by the SWGDE. This makes them more reliable than ordinary witnesses. Crouch (2010) supports this by stating quality control will ensure results of expert finding will be replicable to any expert using the same tools to search for evidence. According to Dougherty (2002), computer forensic expert should be used to search and preserve computer evidence because of their capabilities to identify intrusion as they are familiar with the places to search and what should be searched for. Forensic experts are able to preserve evidence from damage, thus, in mechanical and electromagnetic, alterations and viruses. Meyers (2005:46) and Meyers and Rogers (2004:6) agree it will be ideal to use computer forensics experts in searching for evidence because they have been subjected to several tests on how they use tools to conduct searches and extraction of information related to computer crime.

Meyers (2005:47) and Meyers and Rogers (2004:6) further explain that the ability to use a tool or software package without explicit explanation on how the tool works or source code does not necessary make one an expert. This is because a software package cannot be regarded as expert. Leach, Vanacour and Bishop (2010:11) and Wall and Paroff

(2004) in their discussions say it is good practice to use a computer forensic expert to search and preserve evidence because he can do the following:

- Analyse forensic image of storage and determine what was stored in the device, dates and how the files were accessed or deleted including establishing what peripheral devices were connected to the device.
- Search a forensic image of a hard drive for fragments of a file or a file that previously existed on the hard drive.
- Able to determine terms used to search the Internet including visited websites, purchased wiping software and utilised.
- Search for a “pst” to locate email messages with specifications to people, words, date, and it enables matching up of attachments with e-mails.
- Locate deleted data files.
- Develop search protocols, procedures for review of a forensic image, and preservation of evidence.

Palmer (2013) agreeing with Leach, et al. (2010:13) Wall and Paroff (2004) illustrates that the computer forensics experts have the ability to search for evidence from entire storages and operating systems using properly defined tools and have the ability to search and retrieve data from seemingly inaccessible media. They can also search and access active data, recover both deleted data and e-mails, search and access inactive data and texts, search and access both encrypted files and passwords, search and obtain information databases and related software. According to Wall and Paroff (2004), computer forensics expert should perform what is viewed as normal collection and preservation of evidence techniques by ensuring that they observe the chain of custody and that their actions do not damage or alter data or mirror imaging.

3.10 LEGAL REQUIREMENTS FOR THE ADMISSIBILITY OF COMPUTER EVIDENCE IN COURT

According to Mukuruba (2013), there is no notable judicial precedence in Zimbabwe on the question of admissibility of computer-related crime evidence. In the matter of Paradza v Chirwa and others 2005 (2) ZLR 94 (S), the Supreme court ruled that, “In any case it is not our law that evidence obtained as a result of an unlawful interception of a telephone conversation should be excluded from use in court proceedings. The rule applicable to courts is that the admissibility of illegally or improperly obtained evidence is a matter for determination by the court in the exercise of its discretion”.The common rule applied in this case serves as a judicial precedence to all electronic evidence cases. It is, therefore, necessary to legislate on the admissibility of electronic evidence to avoid it being classified as “improperly obtained evidence”. The steps adopted thus far with regards to the admissibility of electronic evidence do not adequately address the gap created by increasing levels of computer related crime and the relevant laws in Zimbabwe.

Watney (2009) states that in the South African legal perspective it is argued that admissibility centres on determining whether electronic evidence is documentary or real evidence before a two-phased procedure is applied in determining the admissibility of the electronic evidence. If it is admissible then the evidential weight is established as provided in the Electronic Communications and Transactions Act 25 of 2002. Regardless of the non-existing laws in Zimbabwe, the researcher looked at the admissibility of computer evidence in other countries. According to the Technology Law Development Group (2003:1-3), in Singapore the Evidence (Amendment) Act 1996 introduced new provisions to the Evidence Act to “facilitate the use of information technology” and to “provide for the admissibility and weight of computer output produced by any computer or network as evidence in both criminal and civil proceedings”. Partner (1997:3) mentions that, in the United Kingdom (UK), admissibility of electronic evidence is provided by Civil Evidence Act 1968 and the Police and Criminal Evidence Act 1984 which elaborates a computer reproduced document shall be admissible provided its authenticity is proved.

On the thirty six dockets perused six cases were, declined to be prosecuted, seven cases were withdrawn and two cases had persons acquitted. Out of the eleven cases where searches were done, nine cases could not secure conviction because of issues related to searching and collection of evidence. Twelve cases were filed after accused persons although known could not be located. Two cases were still on the court roll. Three cases recorded convictions and four cases were filed undetected. According to Thomson (2011:7), in the majority of legal proceedings the foundations for digital are determined by principles of authentication and admissibility derived from the use of paper evidence. Thomson (2011:7) and Partner (1997:3) further list five evidentiary issues that will see the admissibility of computer evidence as:

- Relevant – evidence must be relevant with abilities to prove or disprove a consequential fact during the trial.
- Authentic – a procedure for determining that digital data or a document is what it is perceived to be.
- Hearsay – evidence must be admissible under the hearsay exception particularly if the records are used as substantive evidence.
- Best Evidence – relevant if the document's contents are at issue and in the absence of originals of digital evidence.
- Probative value must outweigh any prejudicial effect – logically relevant evidence may be inadmissible if its probative is outweighed by unfair prejudice or irrelevant presentations.

Thomson (2011:7) further lists three fundamental challenges to authenticity of digital records as; identity management challenge related to the author of the records, the reliability of the computer that generated the computer and alteration, manipulation and damaged records after their creation. Reeds (2005:8) and Thomson (2013) present three reasons that may render a record produced by a computer inadmissible as evidence. The three reasons are; because the record is not original, it is hearsay and some rule of law may impede the evidence from being adduced in a court of law. However, Reeds (2005:9) concludes that documents produced by a computer will be admissible to prove a fact, that

is, if the document was produced by the computer during its regular operation for business over the period in issue and the information in the statement was regularly supplied to the computer over that period. Reeds (2005:9) further emphasizes that documents will also be admissible if, during that period the computer operated properly and when not in operation it did not affect the accuracy of the document, and information reproduced is derived from information supplied to the computer in the ordinary course of duty. Reeds (2005:12) and Vella (2013) are of the opinion that in authenticating evidence so that it is admissible, there is need to prove that there is no change to the contents of the record, the contents in the record originate from the purported source, and that inconsequential information such as date of the record is accurate.

Walker (2005:2) mentions the Fed. R. Evid. 803(6) (Exception to the rule against hearsay) test of admissibility is governed by federal courts judicial precedence. Computer records are accepted as business records if they remain in pursuit of routine for motives that tend to assure their accuracy. There are two categories of computer records, thus, the computer-generated and computer stored. Partner (1997:3) says computer stored records, if presented to prove the truth of the matter must comply with hearsay rule and show that human statements contained therein are reliable. In contrast, computer-generated records consist of output of computer programs without human statements. Freeman (1998) gave an example of admissibility of computer records as evidence in the matter of *Kennedy v. Los Angeles Police Department*, 1989 by Ninth California Court of Appeals (901 Federal Second pp. 702–716), in this matter computerized billing records were adduced as evidence and the proof of safeguards to ensure their integrity and were rendered admissible. Frieden and Murray (2011:2) mention that whilst electronic evidence has unique challenges to admissibility and authenticity it still requires the person searching and presenting it to retain knowledge of traditional evidentiary fundamentals as this will lead nearly to the correct result.

3.11 PRESENTATION OF COMPUTER EVIDENCE IN COURT

According to Madhuku (2010:73-74), a court may fail to deliver justice, by failing to appreciate the specialist aspects of an issue. It may have to rely on conflicting expert evidence. This is avoided only if expert witnesses, sensitive to any specific issues relevant to computer related crime and, capable of giving evidence from an informed perspective testify. Hershensohn (2005), posits, the investigator has to give computer evidence viva voce but the challenge is that he will have to translate technical terms to the court. Sherman (2006) further asserts that the investigator should use communication strategy so that lay people can make an informed decision. Gonzales, Schofield and Hagy (2007:39) and Kessler (2010:88) agrees that the issues listed below are guidelines of successfully presenting computer evidence in court.

- Educating the audience; enlightening the court of complex issues related to computer-related terminology throughout the litigation process (Gonzales et al. 2007:40).
- What needs to be proved or disproved; the process proving or disproving all digital evidence alternative explanations, (a) These consist of technical anomalies related incomplete or unclear explanation found for a particular anomaly in the evidence, (b) Disproving alternatives is guided by the involved issue and the strength of the case entirely, (c) Timing is everything in rebutting the defence assertion particularly related to the knowledge of the computer (Gonzales et al. 2007:41).
- Expert witnesses and technical evidence; this involves (a) deciding whether a technical expert witness is needed in complex matters of search and examination of computer evidence where an opinion is offered, (b) using both technical fact and expert opinion witnesses effectively, (c) Identification of qualified technical community experts (d) Explaining legal constraints for examining the available evidence. (e) Put in place plans to deal with a Daubert gate keeping challenges and (f) Preparation of witness to testify in digital evidence in examination in chief, cross examination and evidence rebuttal.
- Recurring issues in computer crime trials; (a) connecting the defendant to the computer, (b) the defendant is aware of the digital evidence on the computer, and (c) tying the defendant to the computer and the computer crime.

- Jury selection; in the United States people with sufficient experience of using computers and able to follow the technical testimony are appointed to the jury (Gonzales et al. 2007:46).
- Presenting complicated and technical issues; (a) Kessler (2010:88) says simplification of technical terms and concepts the courts can understand, (b) Sherman (2006) and Gonzales et al. (2007:48) indicate use of aids such as pictures, drawings, and graphs to explain complex systems and concepts, (c) Enhance the court's knowledge through guiding statement through each layer of witnesses' testimony, (d) Technological concerns related to presentations must be reviewed (Gonzales et al. (2007:48).
- Closing argument consists of (a) reminders and (b) relevant points to remember in digital evidence (Sommer, 2012:33).

Thirty participants from sample A, when asked on the presentation of computer evidence in court mentioned that evidence should be given viva voce and must pass a variety of tests such as cross examination. This guidance emanated from section 194 of the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004.Three participants from sample B said computer crime evidence must instead pass a variety of admissibility tests such as best evidence rule and the rule against hearsay. On the thirty six dockets perused, nineteen cases were referred for prosecution in which six cases were, declined to be prosecuted, seven cases were withdrawn and, two cases had persons acquitted. Out of eleven cases where searches were done, nine cases could not secure conviction because of issues related to searching and collection of evidence. There were convictions in three cases.

The researcher agrees with the participants but shares the same views with Gonzales et al. (2007:26) and Sommer (2012:30) who point out that, in presenting the computer evidence in court the investigators should arrange and ensure that: exhibits for presentation are clean copies, there is adequate setup time, there should be deactivation of standby mode, startup screen and screen savers, and there should be audit trail of

presentation such as cueing. Gonzales et al. (2007:26) and Sommer (2012:30) further indicate that referenced exhibits must be fully described as part of the court record and persuade the court to accept nontraditional means of recording the presentation of evidence through videotape, computer presentations, printouts of screen captures and CD-ROMs. Association of Chief Police Officers (APCO) (2009:29) reiterates that, as in certain setups, courts are not equipped with facilities to view images from a DVD or CD-ROMs. Evidence will have to be transferred onto a video or temporary computer facilities that are installed. The exhibit books should also be made available. Sommer (2012:30) concurring with Sherman (2006) and Gonzales et al. (2007:26), mention power point as one of the comprehensive tool of presenting intricate processes in court. This is because graphics can be easily understood as compared to computer diatribe (Kessler, 2010:88).

3.12 CHALLENGES FACED BY INVESTIGATORS IN DEALING WITH COMPUTER EVIDENCE.

According to Kunz and Wilson (2004:3), the absence of a uniform method of defining computer crime helps provide unending challenges to investigators. Kunz and Wilson (2004:37) and United Nations Office on Drugs and Crime, (2005) assert that this is further compounded by jurisdictional challenges as unlike traditional crimes. Computer-related crimes at times cross boundaries and borders. Investigators are, therefore, faced with challenges of searching for computer evidence or executing search warrant outside their jurisdiction as they are not equipped to extraterritorialities of computer crime. There is lack of international cooperation (United Nations Office on Drugs and Crime, (2005). United Nations Office on Drugs and Crime, (2005) further add that intangible and transient computer-related crime evidence provides a daunting task to investigators because it is volatile and short-lived. Collier and Spaul (1992) and Farmer and Celentano (2000:122) identified the primary challenges encountered by investigators in dealing with computer crime as the investigator's competence in searching for computer evidence, the definitions and computer-related crime terminologies. They also *cited* evidentiary problems related to jurisdiction and deficiencies in laws dealing with the searching of

computer-related evidence and, finally, insufficient resources allocated to investigators who search and seize computer- related crime evidence.

Twelve participants from sample A, when asked of challenges faced by investigators in dealing with computer evidence said the search of digital evidence is the first process that is commonly disputed in court cases and it poses a great challenge to the investigators. Ten participants from sample A argued that it is difficult to plan a computer search because the search procedures are more contingent than procedures for physical searches and they are more of an art than a science. Eight participants from sample A indicated that encryption is a challenge to forensic investigators because it uses a key to hide or conceal information. Three participants from sample B said other challenges that investigators face is that digital evidence can be preceded by a suppression hearing when the courts determine the reasonableness of the search and that it did not violate anyone's rights. The researcher agrees with the foregoing assertion and presents that the challenge is the absence of standardization of the procedures for gathering, handling, transporting, access and documentation.

Etter (2001:27), Sen (2001:65) and Farmer and Celentano (2000: 122) state that the unique nature of electronic evidence poses a new challenge to investigators such as:

- Anonymity of the offender;
- Global reach of computer evidence against capabilities for searching computer-related evidence at a larger scale.
- Computer-related crime is committed at a high speed yet searching and collecting evidence by investigators may require substantial time.
- Deliberate exploitation of issues related to sovereignty and jurisdiction by criminals making searching and collection of computer evidence a challenge.
- The absence of evidence such as eye witnesses and the volatility nature of computer-related crime evidence coupled with high costs of executing investigations.

United Nations Manual on the prevention and control of computer-related crime (1999) discusses the international element in the commission of computer-related crime. Farmer and Celentano (2000:122) agree with the foregoing and say computer systems may be accessed in one country, yet the date manipulates in another country and the repercussions recorded in a third country. Searching for evidence in networks and data bases in different continents is unachievable. United Nations Manual on the prevention and control of computer-related crime (1999) maintains that, regardless of the international laws, the speed and mobility of electronic evidence provides challenges to the laws. According to Sen (2001:59), computer related crime evidence is of unusual nature and indicates that outmoded laws, jurisdictional and statutory impediments aggravate the challenges. Kunz and Wilson (2004:37) agree with Sen (2001:59) and Farmer and Celentano (2000:122) that non-existence of geographical boundaries of computer crime inhibits investigators to search and collect computer-related crime evidence. This, they argue, is exponentially increased by internet. Sen (2001:80) mentions that other challenges includes all the impediments related to jurisdictional issues in which searches should be done in accordance with the laws of evidence that takes cognizance of collecting and preserving carefully and preserved appropriately.

3.13 SUMMARY

The investigators in computer-related crime should define the procedure for searching computer devices and its peripherals used to commit crime. The search warrant should also seek authority to create a mirror image of a device for use in an off-site search. Searching for computer-related crime evidence is extremely technical and in most instances requires a computer forensics expert and this may be impossible to ascertain before the search. Computer-related crime evidence is vulnerable to inadvertent or intentional modification or destruction and requires a controlled environment to complete accurate search and analysis. The search warrant should be crafted such that it authorizes the temporary removal of computer and its peripherals including passwords so that a computer forensics expert can search for evidence in a laboratory. In the next chapter the researcher will outline the research findings and the recommendations.

CHAPTER 4: FINDINGS AND RECOMMENDATIONS

4.1 INTRODUCTION

The aim of this research was to analyse the manner in which Zimbabwe Republic Police Criminal Investigation Department investigators execute the procedures for searching of evidence during investigation of computer-related crime with the intention to improve admissibility of such evidence.

To address the aim and seek for answers, the researcher formulated two research questions:

- What does computer-related crime entail?
- How are searching procedures executed during investigation of computer- related crime for evidence to be admissible in court?

4.2 FINDINGS

The following are the findings of the research:

4.2.1 Research question 1: What does computer-related crime entail?

4.2.1.1 The research established that computer-related crime is any violation of criminal law that involve knowledge of computer technology for their perpetration, investigations, or prosecution. The findings are that, there seems to be no global uniformity in laws governing computer-related crimes. It was evident that essential elements are extracted from judicial precedencies and, therefore, an attempt to match essential elements may be a conduit in the creation of an identical definition of computer-related crime. The research found that the definitional distinctions of computer-related crime depict differences in addressing computer-related crime. What complicates the definition of computer-related crime is that, what could be classified illegal in one country may not be the same in another. Similar forms are developed to address both computer-related crime and traditional crime through technology. This is because of recursive process inherent in their modification. The researcher concluded that all-inclusive definition continue being elusive. Analysts have

attempted to frame the essential elements of computer-related crime with restricted consensus. The prevailing definitions vary significantly depending on the legislative enactment or institution defining computer related crime. The violation of information and communication technology by criminals is fungible and diversely referred to as computer crime, computer-related crime, cyber-crime, high technology crime, or technology-enabled crime.

4.2.1.2 It was proven that, computer forensics is analytical and investigative techniques used for the identification, preservation, extraction, documentation, interpretation and analysis of computer media which is stored or encoded for evidentiary and root cause analysis. The scientific methods used should be accepted and they will make evidence incontestable in court. The word *forensics* means "to bring to the court." Computer forensics is a new phenomenon in Zimbabwe and there is limited standardization and consistency in the courts of law. The researcher concluded if sound computer forensics is applied it will ensure that evidence collected is not altered, as access to it is restricted to competent persons and that any handling of evidence is documented.

4.2.1.3 There are two types of crime scenes, thus primary scene, which is the environment in proximate of the occurrence within which evidence may be found. The secondary scene as an area, although not in the immediate proximity of the primary crime scene, may still afford evidence thereby connecting the suspects and victims to the crime. The researcher concluded that whilst primary crime scenes are rich in utilizable evidence it is also possible to commence investigations at a secondary crime scene and be led to the primary crime scene and subsequently to suspects or further evidence. The current technology used in the investigation of computer-related crime scene enable investigators to reach conclusions that would have been difficult to achieve using traditional means.

4.2.1.4 The researcher established that, whilst in Zimbabwe only the state police had the mandate to investigate, the Zimbabwean laws also provided for private

investigators.The researcher concluded that investigation mandate outlines the right of the investigators in relation to interviewing parties and collection of evidence for such purposes. The methods, code of conduct and ethics in relation to the investigation should be established prior to the investigation. The allegation must also be within the scope of the mandate.

4.2.1.5 The research established that computer related crime investigator should be familiar with proper means of obtaining, preserving and analysing computer evidence and other pertinent data. The researcher also concluded that, computer-related crime investigator should possess the desideratum appreciation, techniques, competencies, philosophies, cognition and understand fully, potential criminal exploitation of computer technology. To sum up, the qualities of an investigator who investigates computer-related crime should entail, communication and Interview skills, control of emotions, honesty and ethics, technical skills and knowledge, knowledge of the law, critical thinking and problem solving, research and writing skills.

4.2.1.6 It is evident that investigator's responsibility is both a reactive process responding to individual crimes and intelligence driven proactive work in targeting suspected individuals or crime. It also includes delivering justice to victims and preservation of life and property. The researcher established that the investigator's responsibility is to uncover leads through evidence search, collection, interview witnesses, analyze findings including technology-related crimes such as computer crime and testify in court. The investigator's responsibility is complex and multi-faceted because of a number of subspecialties that exist.

4.2.1.7 The research findings are that the research objective of investigation is to:

- Uncover crime.
- Identify, profile and determine suspects.
- Establishing, noting and processing evidence whilst observing all legal admissibility concepts.

- Apprehending the perpetrators whilst observing the statutory concepts provided by and in accordance with the constitution.
- Recovering property in conformity to appropriate searching and seizure procedures.
- Prepare for trial including completing accurate documentation.
- Securing conviction of the accused through testimony and presentation of legally obtained evidence and statements.

The researcher concluded that the objective of the criminal investigation is to establish that a criminal act was committed and then identify and apprehend the offenders using modern technology and forensic sciences.

4.2.1.8 The research conclusion in this area is that the purpose of investigation is achieved when there is apprehension and prosecution of offenders. This will manage and reduce crime. This process will see offenders removed from the environment and circumstances where they are prone to commit crimes and are afforded rehabilitative environment. It also eliminates recidivism.

4.2.1.9 In comparing the types of evidence, the researcher concluded that there is a difference between evidence in a computer-related crime and traditional forms of evidence. This is because computer-related evidence is intangible and mostly it is an electronic pulse or magnetic charge. The researcher acknowledged that the types of evidence that relate to computer crime investigations were direct, real, documentary, and demonstrative.

4.2.1.10 The research established that evidence to be looked for at the computer related crime include physical evidence, such as the computer itself, peripherals, notepads, or documentation, in addition to computer-generated evidence which is a representation of the original evidence. Computer generated evidence is listed as:

- Visual output on the monitor.
- Printed evidence on a printer
- Printed evidence on a plotter.

- Film recorder which may consist of magnetic representation on disk and optical representation on Compact Disk (CD).

Computer related crime evidence can be internet-based and or, in stand-alone computers or devices, including mobile devices. In most cases these have various evidence-gathering methods and tools. The researcher concluded that legally computer-generated evidence is deemed to be hearsay. This is because magnetic charge of the disk or the electronic bit value in memory, which represents the data, is the actual and original evidence.

4.2.1.11 The research established that there is no difference between computer evidence and document evidence as digital evidence is governed by the same rules and laws that apply to documentary evidence. In court a document or a statement contained in the document produced by a computer is admissible as evidence, as long as it was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.

4.2.1.12 Literature says computer-related crimes fit within traditional criminal law categories as computers can be used to commit traditional crimes such as terrorism, copyright infringement fraud, theft, espionage or pornography. The researcher concluded that traditional crime only takes a new dimension when a computer is used to commit the crime, although computer-related crime involve crossing boundaries and borders not seen in traditional crimes. In some instances computer-related crime present unique forms of criminal conduct that bear no conformity to common law or existing crimes. In most cases the production of electronic evidence has become vital in proving the guilt of the accused. The judicial mindset shift has motivated most legal systems across the world to amend their laws because of this inevitable change. Electronic records are now considered to be documents and treated as primary evidence

4.2.1.13 In concluding the ways in which computer is used in crime, the researcher's findings depicted three activities:

- The use of a computer as a target of criminal activity.

- The use of a computer as a tool or instrument used to commit a criminal activity.
- The use of a computer as incidental to the criminal activity.

4.2.1.14 The research established that classification of computer related crime is drawn from the definition of computer-related crime. The researcher concluded that computer crimes are classified according to the computer's role in the commission of the crime first, with the computer being the object, subject of a crime or the instrument used for perpetrating traditional crimes. The literature sectored computer-related crime in four categories as:

- Computer-related crime against individual through computers or networks.
- Computer-related crime against property of a person.
- Computer-related crime against organization and includes banks or service sectors.
- Computer related crime against society.

4.2.1.15 Research established that investigators should do the procedures outlined below at the computer related crime scene;

- Following the identification of scene of computer-related crime the investigator should secure and note every person present at the scene of crime and their roles.
- The investigator should identify all the potential evidences including conventional physical evidences like the manuals, user guides, passwords on slips and bank account numbers. Note the position of the various peripherals.
- The investigator should identify all the perishable evidences and arrange for preservation without disturbing or altering the condition of electronic evidences.
- The system that is already OFF should not be turned ON. If systems are on, they should be left ON.

- On systems that are ON, the investigator should photograph them and document them before technical personnel assists in seizing the evidence.
- The investigator should note all the attached network cables and power lines to the systems and all the network connections, modems, telephone lines and, mark the equipment connection from end and from the source in the walls.

4.2.1.16 The research established that investigation models aid in developing new techniques and tools for investigators. They depict how the information flows in an investigation thereby taking cognisance of the entire computer-related crime investigative process including the digital evidence processing activities. The investigation processes, creates abilities to extract the basic common investigation stages that are allotted among models. The diversion is in the content of each stage where a particular scenario may require different levels or types of details steps. It serves as a good starting point for the development of computer related crime investigation methodology.

4.2.2. **Research Question 2: How are searching procedures executed during investigation of computer-related crime for evidence to be admissible in court?**

4.2.2.1 The research established that a search occurs when an anticipation of privacy that society regards reasonable is transgressed and is viewed as constitutional if it does not infringe a person's reasonable, or legitimate apprehension of privacy. Investigators must ensure that search is within the confines of law. The researcher concluded that, if the investigator does a visual observation into the interior of a home, or require a person to open a door so that the investigator has visual access of the interior of the house, that may constitute a search even if there is no physical entry.

4.2.2.2 The findings of the research are that the tools used for searching computer related evidence should possess divers software in the form of backup, decryption, authentication, log file auditing, disk editing, IP tracking, file

examination and data recovery. Appropriate decision on specific tools for computers to be used is necessary to so that evidence is correctly analysed

4.2.2.3 The eleven out of thirty six dockets where searches were done did not depict how they were conducted. It was evident from the research that investigators require a warrant which is a compelling power authorizing them whilst observing the rights of citizens to enter into a location to search evidence of crime. The researcher concluded that search warrants must distinguish the scope of the search, meaning the investigators should search only for materials that are depicted in the search warrant and authorised by such search warrant. There is need to understand the role played by the computer has played during the commission of the offence consider questions such as; is there probable cause to seize hardware? Is there probable cause to seize software? Is there probable cause to seize data?

4.2.2.3.1 The research findings are that off-site search occurs when investigators retrieve computers, documents, files, and programmes, to an off-site location for a search. The researcher concluded that this is done because digital evidence recovery and applicable logistics cannot be achieved on-site.

4.2.2.3.2 The research established that the exceptions to search without warrant are: exigent circumstances, consent searches, plain view searches, and searches to do a lawful arrest. The findings were that search and seizure can be done without a search warrant if the person concerned consents to the search or if the investigator, on reasonable grounds, believes that a warrant would be issued to him and delay in obtaining a warrant would prevent the seizure or defeat the object of the search.

4.2.2.3.3 The literature says “consent” means willingly agreeing to make an intelligent choice to approve something proposed by another to a person in the possession of and who exercises sufficient mentality. It is evident from the research that consenting party must be informed and serves a right to refuse to give consent. Section 51(1) (a) (b) of the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004, says a police officer may, without warrant, search

any premises for the purposes of seizing any article if the person concerned consents to the search. The search and seizure of the article in question can also be done without consent of the person concerned, if he has reasonable grounds that, a warrant would be issued should he apply for it and that, the delay in obtaining a warrant would defeat the object of the search.

4.2.2.3.4 It has been found that plain view concept occurs during execution of a search warrant when evidence not mentioned in the search warrant surfaces and is seized. The research found that its applicability in computer searches is limited by forensic tools. It is accepted where the crime is serious and it poses challenges when applied in digital environment.

4.2.2.4 The existing searching procedures of physical objects under the Zimbabwe Criminal Procedure and Evidence Act, 14 of 2004 were also applicable to intangible objects. The researcher concluded that the existing law in Zimbabwe does not clarify the distinction between tangible and intangible so as to explicitly define unique aspects of searching intangible data. Therefore, the investigator, using traditional powers to secure data, faces challenges related to access to the computer system, intangible nature of data and data may be stored in another connected system located away from the premises being searched.

4.2.2.5 The research findings were that prior to searching there is need to identify the targets of crime, the computer systems to be searched and software, hardware, networks employed by the targets and methods to be used in searching for evidence. A team should be established that includes investigating officer and computer forensic experts.

4.2.2.6 The thirty six dockets perused did not show that software tools were ever used in retrieving evidence. The research has shown that software used to search for evidence should be appropriately licensed otherwise its use will be successfully challenged in court. Tools should be tested for accuracy, uniformity and for their operability, including both open and closed source testing. The literature says, as a requirement for admissibility, there is need for the tools to be subjected to calibration, peer review and error rates.

4.2.2.7 A chain of custody identifies changes in the control, handling, possession, ownership and custody of piece of evidence and audit trail of the route that the evidence took from the time it is collected until it is presented in court. Chain of custody reduces the chances of evidence contamination, tempering and accounts for all persons who handled or who had access to the evidence in question. The researcher concluded that digital evidence is considered as valid if the chain of custody can demonstrate where, when and who came into contact with electronic evidence in each stage during the investigation.

4.2.2.8 The research has shown that it is vital to use experts as they have comprehensive techniques and knowledge of formats in which evidence can be searched. They have capabilities of making the necessary backups without eliminating or tampering with evidence. It became evident that in court, opinion of an expert witness is admissible as evidence in cases where lay persons are incapable of presenting correct judgment upon the matter that requires scientific knowledge, a previous habit or experience or study.

4.2.2.9 The research established that the steps adopted thus far with regards to the admissibility of electronic evidence do not adequately address the gap created by increasing levels of computer-related crime and the relevant laws in Zimbabwe. This was evident because out of the eleven cases where searches were done nine cases could not secure conviction because of admissibility issues related to searching and collection of evidence The researcher concluded that it is necessary to legislate on the admissibility of electronic evidence to avoid it being classified as improperly obtained evidence.

4.2.2.10 The research established that the investigator should use communication strategy so that lay people can make an informed decision. He should educate the audience, enlightening the court of complex issues related to computer-related terminology throughout the litigation process. He needs to explain what needs to be proved or disproved including the process of proving or disproving all digital evidence alternative explanations. Investigator must pass a variety of tests including cross examination. The researcher concludes that it will also

be ideal to make use of aids such as pictures, drawings, and graphs to explain complex systems and concepts.

4.2.2.11 The research found that investigators are faced with challenges of searching for computer evidence or executing search warrant outside their jurisdiction as they are not equipped to address extraterritorialities of computer crime. Intangible and transient computer-related crime evidence provides a daunting task to investigators because it is volatile and short lived. It is evident that investigators lack competence in searching for computer evidence and there are evidentiary problems related to jurisdiction and deficiencies in laws dealing with the searching of computer-related evidence. There are insufficient resources allocated to investigators who search and seize computer-related crime evidence. The researcher concluded that computer-related crimes are committed at a high speed yet searching and collecting evidence by investigators requires substantial time.

4.3. RECOMMENDATIONS

4.3.1 Bulawayo Metropolitan Criminal Investigation Department as Zimbabwe Republic Police (ZRP) should influence the legislators to establish laws that are comprehensive to address computer related crime. Zimbabwe Criminal Law (Codification and Reform) Act 23 of 2004 promulgated to address computer-related crime does not mention computer-aided crimes as direct crime and lags behind in addressing the actual practice of computer-based crime much more than in other crimes.

4.3.2 The Bulawayo Metropolitan Criminal Investigation Department as ZRP should engage legislators to amend the Zimbabwe Criminal Procedure and Evidence Act 14 of 2004 so that it explicitly permit search and seizure of intangible materials.

4.3.3 The Criminal Investigation Department should eliminate impediments in their criminal investigation procedures manual by strengthening procedures concerning computer-related crime investigation and align it with current trends or with options for continuous amendments.

4.3.4 The Bulawayo Metropolitan Criminal Investigation Department training model should remodel to include aspects of computer-related crime investigation, including search and seizure, examination, analysis, and reporting.

4.3.5 The Bulawayo Metropolitan Criminal Investigation Department should train all investigators in the basics of computer-related crime investigations to meet the demands of the continued advancement in myriad technological, societal and legal issues. This technological growth will in future require all investigators to be familiar with computer crime investigations.

4.3.6 The Bulawayo Metropolitan Criminal Investigation Department computer crime investigators should be trained on legal requirements and correct procedures when searching for evidence during the investigation of computer-related crime. This will enhance their effectiveness in investigating computer-related crime.

4.3.7 Bulawayo Metropolitan Criminal Investigation Department should train investigators to include information relating to searches conducted and how they were conducted in the docket.

4.3.8 Bulawayo Metropolitan Criminal Investigation Department ought to train investigators to appreciate types of evidence, digital evidence, and software used to collect such evidence and admissibility on various kinds of computer evidence.

4.3.9 Bulawayo Metropolitan Criminal Investigation Department should train investigators on the thresholds and legal requirements for issuing a search warrant and exceptions to search without a warrant and how they apply to computer-related crime.

4.3.10 The Bulawayo Metropolitan Criminal Investigation Department as ZRP should adopt good practices from other countries that have computer crime investigation manuals in place.

4.3.11 ZRP ought to recruit experts in the investigation of cybercrime.

4.3.12 Bulawayo Metropolitan Criminal Investigation Department should ensure that search and collection of computer-related evidence is done by trained personnel so that evidence is accepted in court.

4.4 **SUGGESTIONS FOR FURTHER RESEARCH**

The researcher's opinion is that it will be ideal to do further research on the listed aspects:

4.4.1.1 Analysis of procedures that should be followed when seizing a computer during the investigations of a computer related crime.

4.4.1.2 The analysis of existing computer-related crime under the Criminal Law (Codification and Reform) Actin Zimbabwe and the need to reform the laws.

4.4.1.3 Evaluation of legal response to computer-related crime.

4.4.1.4 Mandate to investigate computer-related crime.

4.4.1.5 How Bulawayo Metropolitan Criminal Investigation Department can improve the skills of investigators employed to investigate computer-related crime.

4.4.1.6 Searches of computer evidence outside the borders of Zimbabwe.

4.5 **CONCLUSION**

The aim of this research was to analyse the manner in which investigators executed the procedures for searching of evidence during investigation of computer-related crime with the intention to improve admissibility of such evidence. The researcher wanted to use the acquired research knowledge to develop good practices and guidelines that will be recommended to Bulawayo Metropolitan Criminal Investigation Department Investigating Officers. The researcher is hopeful that the foregoing recommendations will improve investigators efficiency in the investigation of computer-related crime and also provide a reliable source for the Bulawayo Metropolitan Criminal Investigation Department.

The researcher is also hopeful that the recommendations will motivate Bulawayo Metropolitan Criminal Investigation Department to approach the legislators to enact computer-related crime laws that are responsive to current trends and abreast with international laws. Computer-related crime is a new phenomenon in Zimbabwe and inter-disciplinary research including all provinces will address the glaring knowledge gap and accountable national policing practices.

REFERENCES LIST

Ademu, I. O., Imafidon, C.O. & Preston, D. S. 2011. A New Approach of Digital Forensic Model for Digital Forensic Investigation. *International Journal of Advanced Computer Science and Application*s, Vol. 2, No.12, 2011 p 175. University of East London, United Kingdom. Available from: http://thesai.org/Downloads/Volume2No12/Paper%2026-A%20New%20Approach%20of%20Digital%20Forensic%20Model%20for%20Digital%20Forensic%20Investigation.pdf. (22 December 2013).

Al-Azhar, M.N. 2010. Standard Operating Procedure of Seizure on Computer-based Electronic Evidence Forensic. *Cop Journal Volume* 3(2). Available from: http://forensiccop.blogspot.com/2010/01/forensic-cop-journal-32-standard.html (21 March 2013).

Alexandrou, M. 2011. *Computer Crime Definition*. Technology Definitions. Available from: www.mariosalexandrou.com/definition/business-process-outsourcing.asp. (15 March 2013).

Al-Fedaghi, S. & Al-Babtain, B. 2012. Modelling the Forensics Process. *International Journal of Security and Its Applications* Vol. 6, No. 4, Computer Engineering Department, Kuwait University. Available from: http://www.sersc.org/journals/IJSIA/vol6_no4_2012/9.pdf . (23 January 2014).

Alifano, C. M. 2005. The Importance of the Crime Scene. Worldwide Law Enforcement Consulting Group, Clifton Park, New York. Available from: http://www.worldwidelawenforcement.com/docs/The%20Importance%20of%20the%20Crime%20Scene1-A.pdf. (04 January 2014).

Alifano, C. M. 2006. Fundamentals of criminal investigation. Worldwide Law Enforcement Consulting Group. Available from: http://www.worldwidelawenforcement.com/docs/FUNDAMENTALS%20OF%20CRIMINAL%20INVESTIGATIONS.pdf . (01 February 2014).

Alkaabi, A. O. S. 2010. Combating Computer Crime: An International Perspective.

University of Southern Queensland. Available from: http://eprints.qut.edu.au/43400/1/Ai_Alkaabi_Thesis.pdf. (27 January 2014).

Ambhire, V.R. & Meshram, B.B. 2012. Digital Forensic Tools. *IOSR Journal of Engineering* Mar. 2012, Vol. 2(3). Available from: http://www.iosrjen.org/Papers/vol2_issue3/D023392398.pdf. (02 April 2014).

Ami-Narh, J.T. & Williams, P. A. H. 2008. Digital forensics and the legal system: A dilemma of our times Edith Cowan University. Available from: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1040&context=adf. (22 November 2013).

Anti-cartel enforcement manual, 2010. Enforcement Techniques Digital Evidence Gathering. Available from: http://www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf. (24 May 2014).

Arunda, H. S. 2014. Rules of hearsay and documentary evidence in Kenya. Available from: http://harrystephenarunda.wordpress.com/2014/05/16/rules-of-hearsay-and-documentary-evidence-in-kenya/. (20 June 2014).

Ask. K. 2006. Criminal Investigation: Motivation, Emotion and Cognition in the Processing of Evidence Department of Psychology Goteborg University. Available from:https://gupea.ub.gu.se/bitstream/2077/676/1/gupea_2077_676_1.pdf. (03 March 2014).

Aslan, M. Y. 2006. Global nature of computer crimes and the convention on cybercrime Ankara Law Review Vol.3 No.2 (Winter 2006), pp. 129-142 Available from: http://dergiler.ankara.edu.tr/dergiler/64/1541/16889.pdf. (24 January 2014).

Association of Chief Police Officers (APCO), 2009. Good practice guide for computer based electronic evidence. Available from: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. (23 March 2014).

Audit and Investigation Guidelines, 2012. United Nations Development Programme. Available from:

http://www.undp.org/content/dam/undp/documents/about/transparencydocs/OAI_Investigations_Guidelines.pdf. (10 January 2014).

Baber, C., Smith, P., Panesar, S., Yang, F. & Cross, J. 2006. Supporting Crime Scene Investigation Electronic, Electrical and Computer Engineering, Birmingham university press, Birmingham. Available from: www.researchgate.net/...Supporting_Crime_Scene_Investigation/.../9fcfd. (23 January 2014).

Bailey-Beckett, S. & Turner, G. 2009. *Triangulation*: How and Why Triangulated Research Can Help Grow Market Share and Profitability: Available from: http://www.beckettadvisors.com/pdfs/09_may_white_1.pdf. (01 September 2013).

Baldwin, H. B. 2011. The Reminder Card Explanation by Hayden B. Baldwin International Crime Scene Investigators Association. Available from: http://www.icsia.org/FCSI/ReminderCard.pdf. (23/ January 2014)

Barata, K. 1999. Understanding Computers: An Overview for Records and Archives. London UK. Available from: www.irmt.org/documents/educ_training/.../IRMT_computer_sys.do. (23 March 2013).

Bassett, R., Bass, L. & O'Brien, P. 2006 Computer Forensics: An Essential Ingredient for Cyber Security. Western Connecticut State University JIST 3(1*). Journal of Information Science and Technology.* Available from: http://www.scribd.com/doc/91511222/Computer-Forensics-an-Essential-Ingredient-for-Cyber-Security. (22 February 2014).

Becker, R. *&* Dutelle*,* A. W. *2013*. Criminalistics, Forensic science, crime and terrorism. Washington, DC: U.S. Available from: http://www.fbi.gov/about-us/lab/handbook-of-forensicservices-pdf. (21 July 2013).

Bennett, W.W. & Hess, M.K. 2004.*Criminal investigation.* 7th edition. Belmont, CA: Wadsworth Thompson.

Braga, A. A. 2008. *Problem-Oriented Policing and Crime Prevention* 2nd. Criminal Justice Press Monsey, New York, U.S.A. Available from:

http://www.popcenter.org/library/reading/pdfs/braga_pop_intro.pdf. (04 March 2014).

Braga, A. A., Flynn, E.D., Kelling, G. L. & Cole, C. M. 2011. Moving the Work of Criminal Investigators Towards crime control, New Perspectives in Policing. Harvard Kennedy School. National Institute of Justice. Available on: Https://www.ncjrs.gov/pdffiles1/nij/232994.pdf. (24 January 2014).

Branigan, S. 2004. High-Tech Crimes Revealed: Cyber war Stories from the Digital Front, Publisher: Addison-Wesley Professional

Brenner, S. W. and Frederiksen, B. A. 2002. Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review Volume 8 | Issue 1 University of Dayton School of Law Johnson-Laird press, Michigan. Available on: http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1186&context=mttlr. (29 November 2013).

Brooks, J. D. 2004. Valid Searches and Seizures without Warrants. Available on: http://www.ncids.org/Defender%20Training/2004%20Fall%20Conference/Exceptions.pdf. (30 October 2013).

Brown, M. F. & Heinemann, B. B. 2001. *Criminal Investigation: Law and Practice*, 2nd edition.

Bui, S., Enyeart, M. & Luong, J. 2003. Issues in Computer Forensics COEN 150 Dr. Holliday. Available on: http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf. (21 January 2014).

Bulawayo Metropolitan, 2012. Zimbabwe Republic Police Service Plan document.

Bulawayo 24 News. 2012. Comment: Cyber Crime on the Increase: *The 24 News* (24 April 2012).

Carrier, B. & Spafford, E. H. 2003. Getting physical with the digital investigation process Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, IN 47907 *International Journal of Digital Evidence Fall 2003, Volume 2, Issue.* Available from:

https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2003-29.pdf. (04 February 2014).

Cassim, F. 2009. Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study. Available from: http://www.nwu.ac.za/files/images/2009x12x4_Cassim_art.pdf. (20 February 2014).

Chawki, M. 2004. *The Digital Evidence in the Information Era* Computer Crime Research Center. Available from: www.pdfstation.com/.../Searching-and-Seizing-Computers-and-Obtaining-Electronic-Evidence-....html. (12 June 2013).

Chawki, M. 2005. A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy. Available from: www.ie-ei.eu/IE-EI/.../CriticalLookattheRegulationofCybercrime.doc. (24 October 2013).

Chik, W. B. 2011. Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore. Available from: http://works.bepress.com/warren_chik/26. (22 November 2013).

Chval, K. G. 2006 Chain of custody. Available from: http://bukugratis.1eko.com/pdf/computer_forensics_chain_of_custody_form/By_Keith_G_Chval_Chain_Of_Custody__Protek__Computer__/15_pdf. (23 January 2014).

Ciardhuáin, S. O. 2004. An Extended Model of Cybercrime Investigations International. *Journal of Digital Evidence Summer* 2004, Volume 3, Issue. Available from: https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf. (23 September 2013).

Coelli, T. 2008. A Guide to DEAP Version 2.1: A Data Envelopment Analysis (Computer) Program. Centre for Efficiency and Productivity Analysis Department of Econometrics University of New England Armidale press, Australia. Available from: http://www.owlnet.rice.edu/~econ380/DEAP.PDF. (13 November 2013).

Cohen, F.B. 1991. A Formal Definition of Computer Worms and Some Related Results. Pittsburgh, PA 15217, USA. Available from: http://all.net/books/tech/wormdef.pdf. (12 December 2013).

Collier, P. A & Spaul, B. J. 1992. PROBLEMS IN POLICING COMPUTER CRIME. Woolwich Centre for Computer Crime Research, University of Exeter, Vol 2, pp. 307-320 0 1992 Harwood Academic Publishers. Available from: www.tandfonline.com/doi/pdf/10.1080/10439463.1992.9964650. (23 January 2014).

Collins, J. M. 2007. Search Warrant application Manual, Municipal Police Institute. Available from: http://www.municipalpoliceinstitute.org/documents/SEARCH_WARRANT_APPLICATIONS_MANUAL_Illustrated.pdf. (23 February 2013).

Craiger, J. P., Swauger, J. & Marberry, C. 2005. Digital evidence obfuscation: Recovery techniques, University of Central Florida press, Florida. Available from: http://www.cyberace.org/Publications/craiger.5778-85.SPIE.pdf. (11 January 2014).

Creswell, J.W. 2003. *Research design: Qualitative, Quantitative and Mixed method Approaches*. (2nd revised Edition) London: sage publications.

Crime Act, 1914 enacted by Parliament of Australia. Available from: http://www.austlii.edu.au/au/legis/cth/consol_act/ca19148. (11 January 2014).

Crouch, J.E. 2010. An Introduction to Computer Forensics. Available from: http://www.nsci-va.org/WhitePapers/2010-12-16-Computer%20Forensics-Crouch-final.pdf. (03 March 2014).

Cyber Crime Investigation Manual, 2011. Data Security Council of India Niryat Bhawan, New Delhi Designed and Printed by Swati Communications. Available from: http://uppolice.up.nic.in/All%20Rules/Cyber%20crime/4-Cyber_Crime_Investigation_Manual.pdf. (23 October 2013).

Dahake, S. & Daware, S. 2012. Study of Digital Forensic: Process and Tools. Published by *International Journal of Computer Applications*® (IJCA) 29.

Available from: http://research.ijcaonline.org/ncipet/number10/ncipet1079.pdf. (02 October 2013).

Daley, M. A. P. 2010. Computer Forensics Duff & Phelps, LLC; Commercial Fraud Manual. Available from: http://www.duffandphelps.com/sitecollectiondocuments/articles/Computer_Forensics_Chapter_3_for_ABI_Commercial_Fraud_Manual.pdf. (21 February 2014).

Davis. J. T. 2010. Computer crime in North Carolina. Assessing the Needs of Local Law Enforcement. North Carolina. USA. Available from: https://www.ncdps.gov/div/gcc/pdfs/pubs/cybercrime.pdf (22 August 2013).

Delhi Special Police Establishment Act, 1946. Available from: http://track.unodc.org/LegalLibrary/LegalResources/India/Laws/India%20%20The%20Delhi%20Special%20Police%20Establishment%20Act%201946.pdf. (23 September 2013).

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

Dougherty, J.J. 2002. Computer Forensics. Available from: http://www.giac.org/paper/gsec/584/computer-forensics/101347. (24 January 2014).

Douglas, J. E., Burgess, A. N., Burgess, A. G. & Ressler, R. K. 2006. Crime Classification Manual. A standard system for investigating and classifying violent crimes second edition published by Jossey-Bass a Wiley Imprint, San Francisco. Available from: http://murders.ru/Classific.pdf. (22 November 2013).

Duhaime, L. 2005. A.G. (Nova Scotia) v. MacIntyre, [1982] 1 S.C.R. 175 Duhaime's Criminal Law Dictionary. Available from: http://www.duhaime.org/LegalDictionary/S/SearchWarrant.aspx. (23 June 2013).

Dykstra, J. & Sherman, A. T. 2012. Understanding issues in cloud forensics: Two hypothetical case studies, University of Maryland press, Baltimore County (UMBC). Available from:

http://www.csee.umbc.edu/~dykstra/DykstraUnderstandingIssuesInCloudForensics.pdf. (01 February 2014).

Etter, B. 2001. The challenge of the forensic investigation of computer crime Australasian Centre for Policing Research. Available from: http://www.afp.gov.au/~/media/afp/pdf/c/comp-crim.ashx. (22 January 2014).

European Convention on cybercrime. Substantive Criminal Law 2001. Available from: http://www.issafrica.org/uploads/MISSIONAPPEND.PDF. (21 January 2014).

Farmer, J. J. & Celentano. L. 2000. Computer Crime Joint Report, New Jersey. Available from: http://www.state.nj.us/sci/pdf/computer.pdf. (22 June 2013).

FBI Law Enforcement Bulletin, 2011. Digital Evidence, Volume 80 Number 8 United States Department of Justice Federal Bureau of Investigation Washington, DC. Available from: http://leb.fbi.gov/2011/august/leb-august-2011. (11 November 2013).

Feltoe, G. 2009. Criminal defender's handbook, International Bridges to Justice, Legal Resource Foundation, Harare, Zimbabwe.

Forensic Examination of Digital Evidence, A guide for law Evidence, 2004. U.S. Department of Justice Office of Justice Programs National Institute of Justice. Available from: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf. (22 February 2014).

Frederiksen, B.A. 2002. Computer Searches and Seizures: Some Unresolved Issues. University of Dayton press. Michigan Telecommunications and Technology Law Review Volume 8 | Issue. Available from: http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1186&context=mttl. (12 November 2013).

Freeman, E. H. 1998 Data security management the use of computer records as courtroom evidence, Auerbach Publications. CRC Press. Available from: http://www.ittoday.info/AIMS/DSM/8203351.pdf. (12 October 2013).

Frieden, J. D. & Murray, L. M. 2011. The Admissibility of Electronic Evidence under the Federal Rules of Evidence, XVII RICH. J. L. & TECH. 5. Available from: http://jolt.richmond.edu/v17i2/article5.pdf. (23 January 2014).

Fourth Amendment and the Privacy Protection Act (PPA) of 1980. Available from: http://epic.org/privacy/ppa/. (23 February 2014).

Forester, T. and Morrison, P. 1991. Computer Ethics: Cautionary Tales and Ethical Dilemmas in computing. Available from: http://jolt.law.harvard.edu/articles/pdf/v04/04HarvJLTech299.pdf?origin=publication_detail. (23 June 2013).

Garfinkel, S. L. 2009. Providing Cryptographic Security and Evidentiary Chain-of-Custody with the Advanced Forensic Format, Naval Postgraduate School and Harvard University, USA. *International Journal of Digital Crime and Forensics,* 1(1), 1-28. Available from: http://calhoun.nps.edu/bitstream/handle/10945/35002/2009.pdf?sequence=1. (21 November 2013).

Gayed, T. M., Lounis, H. & Bari, M. 2012. Cyber Forensics: Representing and (Im) Proving the Chain of Custody Using the Semantic web. Available from: www.thinkmind.org/download.php?articleid=cognitive_2012_1_40. (02 March 2013).

General instructions regarding investigation & enquiries. 2013. Available from: http://cbi.nic.in/aboutus/manuals/crimemanual.php. (27 December 2013).

George, A. 2011. *Research in Practice for adults, Research Guide.* Available from: http://www.chnri.org/resources/2.%20Research%20Methodology/Topic%203%20Formulating%20Research%20Question/Research%20Guide%20Developing%20research%20questions.pdf. (19 March 2013).

Ghosh, A. 2004. Guidelines for the Management of IT Evidence Incident Response and Forensics Workshop; Australia Guidelines for the Management of IT Evidence APEC Telecommunications and Information Working Group 29th Meeting, Hong Kong, China. Available from:

http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf. (19 November 2013).

Giova, G. 2011. Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems. IJCSNS *International Journal of Computer Science and Network Security*, VOL. 11 No. 1.Available from: http://paper.ijcsns.org/07_book/201101/20110101.pdf (28 December 2013).

Golafshani, N. 2003. *Understanding Reliability and Validity in Qualitative Research*. University of Toronto press, Toronto, Ontario, Canada. *The Qualitative Report* Volume 8, 597-607. Available from: http://www.nova.edu/ssss/QR/QR8-4/golafshani.pdf. (02 May 2013).

Gonzales, A. R., Schofield, R. B. & Hagy, D. W. 2007. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U.S. Department of Justice Office. Available from: https://www.ncjrs.gov/pdffiles1/nij/210798.pdf. (28 January 2014).

Goodman, M.D. 1997. Why the Police don't care about computer crime, Harvard *Journal of Law and Technology*. V 10, Number 3. Available from: http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf. (01 May 2013).

Gray, D. 2008. Forensic Accounting and Auditing: Compared and Contrasted to Traditional Accounting and Auditing, *American Journal of Business Education – Fourth Quarter* 2008 Volume 1, Number 2 Loyola College, USA. Available from: http://www.cluteinstitute.com/ojs/index.php/AJBE/article/viewFile/4630/4719. (11 September 2013).

Guide for Virginia Law Enforcement Agencies, 1997. Crime Prevention Standards. Virginia Crime Prevention Association 1405 Westover Hills, Richmond. Available from: http://www.theiacp.org/portals/0/pdfs/Crime%20Prevention%20Standards%20-%20VA.pdf. (23 April 2013).

Gunter, W.D. & Hertig, C.A. 2005. An introduction to theory, Practice and Career Development for Public and Private Investigators. International Foundation for protection of Officers.

Hagan, F.E. 1997. *Research Methods in Criminal Justice and Criminology.* 4th edition. Allyn and Bacon: London.

Hana, R. O. A., Freitas, C .O. A, Oliveira, L. S. & Bortolozzi, F. 2008. Crime Scene Classification. Pontifical Catholic University of Paraná press. Available from: http://www.inf.ufpr.br/lesoliveira/download/JUCS2008d.pdf. (29 December 2013).

Harvey, R. 2011. The independence of the Prosecutor a Police perspective', New South Wales Police Service. Available from: http://www.aic.gov.au/media_library/conferences/prosecuting/harvey.pdf. (03 March 2014).

Hershensohn, J. 2005. I. T. Forensics: The collection and presentation of digital evidence. Available from: http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf. (22 January 2014).

Hinduja, F. S. 2007. Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to address the future. *Florida International Journal of Cyber Criminology* Vol 1 Issue 1 Atlantic University. Available from: http://www.cybercrimejournal.com/sameer.pdf. (11 October 2013).

Hollinger, R. C. 2000. Computer Crime, University of Florida press, Gainesville. Available from: http://web.clas.ufl.edu/users/rhollin/Computer_Crime.pdf . 15 December 2013).

Home Office Cyber Crime Strategy. 2010. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf. (31 January 2014).

Homel, R. 1994. Can police prevent crime? School of Justice Administration Griffith University press, QLD. Available from: http://www.griffith.edu.au/__data/assets/pdf_file/0006/188727/can-police.pdf (23 March 2014).

Huebner, E., Bem, D, & Bem, O. 2007. Computer Forensics – Past, Present and Future. University of Western Sydney, School of Computing and Mathematics press, Sidney. Available from: http://cracking8hacking.com/cracking-

hacking/hacking/Computer-Forensics-and-Incident-Handling/Computer_Forensics_Past_Present_Future.pdf. (04 January 2014).

Icove, D., Seger, K. & Vonstroch, W. 1995. Computer Crime a Crime fighter's Handbook Publisher: O'Reilly Media Released: Pages: 464.

Information Security and Forensics Society (ISFS) 2004 Computer Forensics Best Practices. Available from: http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf. (10 January 2014).

Jakob, A. 2001, *On the Triangulation of Quantitative and Qualitative Data in Typological Social Research*, Volume 1. Availablelle from: http://www.beckettadvisors.com/pdfs/09_may_white_1.pdf. (01 April 2014).

Jarrett, M. H. & Bailie, M.W. 2009. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Available from: http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf. (30 November 2013).

John, L. J. 2012. Digital Forensics and Preserving. Digital Preservation Coalition Published in association with Charles Beagrie Ltd. Available from: www.dpconline.org/comp**one**nt/docman/doc.../810-dpctw12-03pdf. (21 January 2014).

Johnson, E. A. 2008. Causal relevance in the law of search and Seizure, Boston university law review vol. 88:113. Available from: http://www.bu.edu/law/central/jd/organizations/journals/bulr/documents/JOHNSON.pdf. (06 May 2013).

Judish, N. 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Available from: http://cdn.ca9.uscourts.gov/datastore/library/2013/02/26/CDT_cyber.pdf. (23 February 2014).

Kadir, R. M. 2010. The Scope and the Nature of Computer Crimes Statutes. *A Critical Comparative Study German Law Journa*l Vol. 11 No. 06. Available from: http://www.germanlawjournal.com/pdfs/Vol11-No6/PDF_Vol_11_No_06_609-632_RM_kadir.pdf. (18 December 2013).

Karn, J. 2013. Policing and Crime Reduction The evidence and its implications for practice, The Police Foundation. Available from: http://www.police-foundation.org.uk/uploads/catalogerfiles/policing-and-crime-reduction/police-foundation-police-effectiveness-report.pdf. (05 February 2014).

Kent, K. Chevaliers. Grance, T. & Dang, H. 2006. Guide to integrating forensic techniques into incident response. National Institute of Standards and Technology. Available from: http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf. (20 September 2013).

Kerr, O. S. 2005. Digital Evidence and the New Criminal Procedure, Directors of the Columbia Law Review Association. Available from:.http://www.prd.uscourts.gov/cle_info/sites/cle_info/files/EventAttachments/digital_evidence.pdf. (16 January 2014).

Kerr. O. R. 2005. Search Warrants in an era of digital evidence. Available from: http://www.olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf. (27 July 2013).

Kerr. O. R. 2005. Searches and Seizures in a Digital World. Available from: http://isites.harvard.edu/fs/docs/icb.topic1020905.files/SearchandSeizureDigital.pdf. (20 September 2013).

Kessler, G. C. 2010. Judges' Awareness, Understanding, and Application of Digital Evidence. Nova Southeastern University press, Nova. Available from: http://www.garykessler.net/library/kessler_judges%26de.pdf. (21 October 2013).

Kohn, M. Eloff, J.H.P. & Olivier, M. S. 2006. Framework for a Digital Forensic Investigation. Information and Computer Security Architectures Research Group. University of Pretoria. Available from: http://mo.co.za/open/umldfpms.pdf. (27 November 2013).

Kunz, K. & Wilson, P. 2004. Computer Crime and Computer Fraud. University of Maryland Department of Criminology and Criminal Justice Fall, 2004 Report to the Montgomery County. Available from: www.montgomerycountymd.gov/content/…/computer_crime_study.pdf. (23 June 2013).

Kurzban, S.A.1995. Authentication of computer-generated evidence in the United States Federal Courts by the PTC Research Foundation of the Franklin Pierce Law IDEA. *The Journal of Law and Technology.* Available from: http://ipmall.info/hosted_resources/IDEA/16.Kurzban.pdf. (23 March 2013).

Kozushko, H. 2003. Digital Evidence Sunday Available from: http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf. (11 April 2014).

Latham and Watkins 2013. Litigation Department. Available from: www.lw.com/thoughtLeadership/search-warrant-steps. (22 July 2013).

Law Commission Report 2007. Computer searches. Available from: http://www.lawcom.govt.nz/sites/default/files/publications/2007/06/Publication_96_358_Part_2_R97%20part-2.pdf. (22 March 2014).

Law Reform Commission, Act 2005. Available from: http://attorneygeneral.gov.mu/English/Documents/A-Z%20Acts/L/Page%201/LAWREFORMCOMMISSION1.pdf. (23 April 2013).

Law reform paper, 2009. Documentary and Electronic Evidence. Available from: http://www.lawreform.ie/_fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf. (29 December 2013).

Leach, S., Vanacour, J. & Bishop, A. 2010. What Every Lawyer Needs to Know About Computer Forensic Evidence. Available from: https://www.utexas.edu/law/journals/tiplj/documents/symposia/2010/Slides/Sid%20Leach%20%20Computer%20Forensic%20Evidence%20in%20IP%20Litigation%20Paper.pdf. (22 January 2014).

Lee, H. C & Pagliaro, E. M. 2013. Forensic Evidence and Crime Scene Investigation. J Forensic Investigation. April 2013 Vol.:1, Issue: 1. Available from: http://www.avensonline.org/wp-content/uploads/2014/01/JFI-2330-0396-01-0004.pdfv. (21 July 2013).

Leedy, D. & Ormrod, J. E. 2010. *Practical Research: Planning and Design.* 8th Edition. Merrill Prentice Hall: Ohio.

Loginsky, P. B. 2011. Confessions, Search, Seizure, and Arrest a Guide for Police officers and prosecutors Washington Association of Prosecuting Attorneys. Available from: http://www.impsec.org/~jhardin/gunstuff/legal/May%202011%20final%20SEIZURE%20AND%20CONFESSIONS.pdf (10 July 2013).

Lytle, M. 2008. Forensic Investigations, University of Texas, Brownsville and Texas College Press. Available from: http://www.utb.edu/vpaa/cla/cj/Pages/ForensicInvestigations.aspx. (13 May 2013).

Madhuku, L. 2010. An Introduction to Zimbabwean Law. Published by Weaver Press and Friedrich-Ebert-Stiftung (FES), Belgravia, Harare.

Maghaireh, A. M. S. 2009. Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence University of Wollongong press. Available from: http://ro.uow.edu.au/cgi/viewcontent.cgi?article=4404&context=theses. (28 November 2013).

Magnin, C. J. 2001. An efficient tool to fight crime in cyber-space? The 2001 Council of Europe Convention on cyber-crime. Available from: http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf. (05 February 2014).

Makulilo, A. B. 2006. The Admissibility of Computer Printouts in Tanzania: Should it be Any Different than Traditional Paper Documents? Available from: https://www.duo.uio.no/bitstream/handle/10852/20801/temp2-1.pdf?sequence=2. (23 March 2013).

Maras, M. H. 2011. Computer Forensics: Cybercriminals, Laws, and Evidence Jones & Bartlett Learning.

Marshall, T., Robinson, T., and Kwak, D. 2005, *Computer Crime in a Brave New World. Handbook of Transnational Crime & Justice*. Ed. Philip Reichel. Thousand Oaks, CA: Sage, Sage Publications.

Marsico, C. V. 2005. COMPUTER EVIDENCE V. DAUBERT: The coming conflict, Purdue University Press, West Lafayette. Available from: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-17.pdf. (21 September 2013).

Masango, C. 1998. Zimbabwe Republic Police, Crime Investigation Manual. Juta, Zimbabwe [Private] Limited.

Masango, C. 2004. Zimbabwe Republic Police, Criminal Law Manual. Juta, Zimbabwe [Private] Limited.

Meeker, J. 2005. SEARCH AND SEIZURE STATE AND FEDERAL LAW Austin, Texas State Bar of Texas. Available from: http://www.yourhonor.com/dwi/SBM/SBM9.pdf. (23 March 2014).

Meyers, M. & Rogers, M. 2004. *Computer Forensics. International Journal of Digital Evidence,* Volume 3, Issue 2. Purdue University. Available from: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf?q=computer. (06 January, 2014).

Meyers, M. 2005. COMPUTER FORENSICS: Purdue University Press, West Lafayette. Available from: https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-28.pdf. (20 December 2013).

Microsoft Computer Dictionary, 2002. Fifth Edition published by Microsoft Press a Division of Microsoft Corporation One Microsoft Way Redmond, Washington Microsoft Corporation. Available from: http://flylib.com/books/en/2.892.1.2/1/. (23 November 2013).

Miller, M. T. 2011. Crime Scene Investigation. Forensic Science: An Introduction to Scientific and Investigative Techniques. 82003 by CRC Press LLC 2011.Aavailable from: http://www.cbsd.org/cms/lib07/PA01916442/Centricity/Domain/1908/CSI%20Text%20Marilyn%20Miller.pdf. (23 February 2014).

Mobbs, P. 2003. Computer Crime. The law on the misuse of computers and networks. GreenNet IR Toolkit Briefing. Available from: http://www.infosyssec.net/infosyssec/compcrim1.htm. (23 April 2013).

Moore, M.H., Trojanowicz, R.C. & Kelling, G. L. 1988. Crime and Policing A Publication of the National Institute of Justice, U.S. Department of Justice, and the Program in Criminal Justice Policy and Management, Harvard University Press, Harvard. Available from: https://ncjrs.gov/pdffiles1/nij/111460.pdf. (02 February 2014).

Mouton, J. 2001. *How to succeed in your Master's and Doctoral Studies*. Western Cape: Van Schaik Publisher.

Mukuruba, R. S. 2013. Support for Harmonization of the ICT Policies in Sub-Sahara Africa (HIPSSA). Available from: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/Incountry%20support%20documents/Zimbabwe%20Cybercrime%20Cases%20Presentation.pdf. (03 April 2014).

Mumbai Police Cybercrime Report, 2004. Crime Brands, CID Mumbai, Crawford Mumbai India. Available from: http://www.justdial.com/Mumbai/Police-Cyber-Crime/ct-253204. (12 February 2013).

Mundt, T. 2009. Computer Forensics–Foundations. Available from: http://basoti.uni-rostock.de/basoti/material/basoti2013/cf/Mundt_L1__Foundations.pdf. (13 January 2014).

Mussio, D. 1990. Drawing the Line between Administrative and Criminal Searches: Defining the "Objective of the Search" in Environmental Inspections College Environmental Affairs Law Review Volume 18 | Issue 1 Article 14. Available from: http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1500&context=ealr. (28 August 2013).

Nandhakumar, N.K., Agarwal, U. & Faizal, H. 2012. Chain of Custody Methodology for Fool proof Computer Forensics. *Operation International Journal of Communication and Networking System.* Volume: 01 Issue: 01 College of Technology Oman-Post. Available from: http://www.ijcnes.com/papers/vol1issue1/ijcnes-vol1issue1/jun-12-ijcnes-006.pdf. (13 June 2014).

Nemeth, C. P. 2013. Law and Evidence, a primer for criminal justice, criminology, law and legal studies, 2nd edition, California university of Pennsylvania. Jones and Bartlett Publishers.

Newby, T., Schwarz, J.M. & Carroll, O.L. 2005. Rethinking the storage of computer evidence, US Department of Justice. Available from: http://www.unafei.or.jp/english/pdf/RS_No79/No79_07VE_Schwarz2.pdf. (10 December 2013).

New Jersey Computer Evidence Search & Seizure Manual Department of Law & Public Safety Division of Criminal Justice April 2000.Available from: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf. (22 February 2014).

Newsom, D. 2006. Computer Forensics – Overcoming the "after-the-fact" approach Proper procedures in computer forensics must be followed in any investigation relying on computer or electronic information, regardless. Available from: http://www.cosmopolitanuniversity.ac/library/ComputerForensics.pdf. (11 April 2013).

Ngafeeson M. 1999. Cybercrime Classification: A Motivational Model. College of Business Administration the University of Texas-Pan American press, Edinburg, USA. Available from: http://www.swdsi.org/swdsi2010/sw2010_preceedings/papers/pa168.pdf. (22 February 2014).

Oates, B. J. 2006. Researching Information Systems and Computing. Los Angeles: Sage Publications.

Olufunke, O. O. 2010. Computer Crimes and Counter Measures in the Nigerian Banking Sector. *Nigeria Journal of Internet Banking and Commerce An open access Internet journal of Internet Banking and Commerce*, vol. 15, no.1m. Available from: http://www.arraydev.com/commerce/jibc/2010-04/OLASANMI-JIBC%20Doc.pdf. (23 December 2013).

Palmer, A. 2013. Computer Forensics: The Six Steps. Available from: http://pencaribuku.vapr.cc/pdf/computer_forensics_jobs_uk/Computer_Forensics_The_Six_Steps_Adrian_T_N_Palmer__/26_pdf. (20 June 2013).

Parker, D. B. 1989. COMPUTER CRIME Criminal Justice Resource Manual U.S. Department of Justice National Institute of Justice Office of Justice Programs. Available from: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf. (24 October 2013).

Partner, J. G. 1997. The admissibility of computer-generated evidence: an overview. Available from: http://www.cmla.org/papers/Admissibility%20of%20Computer%20Generated%20Evidence.Johanne%20Gauthier.28.Nov.1997.pdf. (12 October 2013).

Patzakis, J. 2003. Accounting Reform Laws Push For Technology-Based Document Retention Practices. *International Journal of Digital Evidence Spring* 2003, Volume 2, Issue 1 New. Available from: www.digital4nzics.com/.../New%20Accounting%20Reform%20Laws%2. (23 April 2013).

Paulsen, N. 2010. *Developing Research Questions* and the PHD, UQ Business School. Available from: http://wmssoros.mngt.waikato.ac.nz/NR/ANZAM/docs/Neil_Paulsen_DevelopResearchQuestions.pdf. (12 July 2013).

Pena, M. S. 2000. Practical Criminal Investigation, 5th ed., Manuel S. Pena, Wadsworth.

Perlmutter, 2013. What is a search Warrant? Long Island and Westchester. Available from: http://adplegal.com/what-is-a-search-warrant/. (12 July 2013).

Perumal, S. 2009. Digital Forensic Model Based On Malaysian Investigation Process. *IJCSNS International Journal of Computer Science and Network 38 Security*, VOL.9 No.8, University Of Malaysia press, Malaysia. Available from: http://paper.ijcsns.org/07_book/200908/20090805.pdf. (20 October 2013).

Philippine National Police Criminal Investigation Manual, 2011. Published by Directorate for Investigation and Detective Management Philippine National Police. Available from: http://didm.pnp.gov.ph/DIDM%20Manuals/Criminal%20Investigation%20Manual.pdf. (02 March 2014).

Pladna, B. 2008. Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them. East Carolina University press, East Carolina. Available from: http://www.infosecwriters.com/text_resources/pdf/BPladna_Computer_Forensic_Procedures.pdf. (21 January 2014).

Quality standards for investigations November, 2011. Council of the Inspectors General on Integrity and Efficiency. Available from: https://www.ignet.gov/pande/standards/invstds2011.pdf. (01 March 2014).

Reeds, C. 2005. The Admissibility and Authentication of Computer Evidence - A Confusion of Issues. Available from: http://www.bileta.ac.uk/content/files/conference%20papers/1990/The%2520Admissibility%2520and%2520Authentication%2520of%2520Computer%2520Evidence%2520-%2520A%2520Confusion%2520of%2520Issues.pdf. (22 October 2013).

Reith, M. Carr, C. & Gunsch, G. 2002. An Examination of Digital Forensic Models *International Journal of Digital Evidence Fall* 2002, Volume 1, Issue 3. Available from: www.researchgate.net/.../2589967_An_Examination_of_Digital_Forensic. (23 August 2013).

Robbins, J. 1994. *Federal Guidelines for Searching and Seizing Computers* US Department of Justice Criminal Division Office of Professional Development and Training. Available from: http://www.knock-knock.com/federal_guidelines.htm. (23 February 2014).

Rossmo, D.K. 2005. Criminal Investigative failures, Centre of Geospatial and Investigations Department of Justice, Texas, State University Press, Texas. Available from: http://www.justice.gov.sk.ca/milgaard/pubdocs/04262006/kim%20rossmo/337674.pdf. (11 March 2013).

Royal Canadian Police Guidelines, 2010. Computer crime, can it affect you. Available from: http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html. (01 March 2013).

Ryan, J. D. & Shpantzer, D. C. 2008. Legal Aspects of Digital Forensics, George Washington University Press, Washington. Available from: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf. (24 April 2014).

Ryder, K. 2002. Computer Forensics – We've had an incident, who do we get to investigate? Certification Assignment Version 1.3 Page 1 of 12. Available from: http://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652. (21 February 2014).

Saboohi, M. 2006. Collecting digital evidence of cyber-crime. International Islamic University press, Islamabad. Available from: http://www.supremecourt.gov.pk/ijc/articles/10/2.pdf. (28 April 2013).

Sady, S.R. 2012. Developments in Federal Search and Seizure Law. Available from: http://or.fd.org/search%20and%20seizure.pdf. (09 March 2014).

Sarrab, M., Aldabbas, M. & Elbasir, M. 2013. Challenges of Computer Crime Investigation in North Africa's Countries. The International Arab Conference on Information Technology. Available from: http://www.acit2k.org/ACIT/2013Proceedings/194.pdf. (24 February 2014).

Schatz, B. 2007. Digital Evidence: Representation and Queensland University of Technology press. Available from: http://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf. (24 April 2014).

Schell, B. & Martin, C. 2006. Webster new world hackers' dictionary. Wiley publishing. Available from: http://www.amazon.com/Websters-New-World-Hacker-Dictionary/dp/B005OLA6S6. (06 January 2014).

Scientific Working Group on Digital Evidence, SWGDE 2006. Best Practices for Computer Forensics. Available from: http://www.oas.org/juridico/spanish/cyb_best_pract.pdf. (06 January 2014).

Sen, O. N. 2001. Criminal Justice responses to emerging computer crime problems. University of North Texas press. Available from: http://digital.library.unt.edu/ark:/67531/metadc2866/m2/1/high_res_d/thesis.pdf. (28 August 2013).

Sheppard, F. & Duranti, L. 2010 The Canadian legal framework for evidence and the Digital Economy: a disjunction? UBC. Available from: http://www.ciscra.org/docs/Sheppard_Duranti_The_Canadian_Legal_Framework_FINAL_REPORT.pdf. (03 January 2014).

Sherman, S. 2006. A digital forensic practitioner's guide to giving evidence in a court of law, Edith Cowan University press, Perth. http://cryptome.org/2014/03/forensic-evidence-in-court.pdf. (04 January 2014).

Shin. Y. D. 2011. *New Model for Cyber Crime Investigation Procedure Journal of Next Generation Information Technology*. Volume 2, Number 2. Available from: http://www.aicit.org/JNIT/ppl/1_JNIT_MAY.pdf. (28 November 2013).

Shinder, D. L. 2002. Scene of the cyber-crime computer Forensic Handbook. Published by Syngress Hingham Street Rockland.

Shipley, T. G. & Reeve H. R. 2006. Collecting Evidence *from a* Running Computer*:* A Technical and Legal Primer for the Justice. Available from: http://www.search.org/files/pdf/collectevidenceruncomputer.pdf. (29 December 2013).

Shuttleworth, M. 2008. Aims of Research: Experiment –Resources.com. Available from: http://www.experiment-resources.com/aims-of-research.html. (23 May 2013).

Simlot, R. & Christopher, C. 2002, Forensic Investigation and crime scenes, Richard Stockton college of New Jersey, Jim Leeds Roads, Pomona. Volume 40 no 2. Available from: http://www.cbdiai.org/Articles/simlot_chris_fall-02.pdf. (21 January 2014).

Singh, K. 2006. *The fundamental of Research methodology and statistics*. New age International (p) limited, Publishers.

Smith, T.W & Hartmann, J. F. 1998 a How-To Guide for an Effective FBI Search Warrant Response Program Kirkland & Ellis. Available from: www.kirkland.com/sitefiles/kirkexp/publications/.../ma-9-search_dfa.pd... (20 December 2014).

Sogbaike, O., David, O.E., Esther, & Victor, O. 2014. Computer Forensics for Law Enforcement, *Journal of Emerging Trends in Engineering and Applied Delta State Polytechnic Otefe-Oghara Delta State, Nigeria.* Available from: http://jeteas.scholarlinkresearch.com/articles/Computer%20Forensics%20for%20Law%20Enforcement%20new.pdf. (20 February 2014).

Solomon, J. & Lattimore, E. 2008. *Computer Forensics* "Electronic Crime Scene Investigation: A Guide for First Responders." Available from: www.nij.gov/publications/crime-guide-219941/chapter7-219941.pdf. (12 June 2013).

Sommer, P. 2013. Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers. Fourth Edition. Available from: http://www.iaac.org.uk/itemfiles/DigitalInvestigations2013.pdf. (25 April 2014)

Stephenson, P. 2000. Investigating computer-related crime, a handbook for corporate investigators. C R C PRESS Boca Raton London New York Washington, D.C. Available from: http://www.documentingreality.com/forum/attachments/f181/38763-investigating-computer-related-crime-investigating-computer-related-crime.pdf. (11 January 2014).

Tavani, H. T. 2000. Defining the boundaries of Computer Crime: Piracy, Break-ins, and sabotage in Cyberspace, Philosophy Department. River College. Available from: http://www.cs.kent.edu/~rothstei/spring_13/papers/CrimeBoundaries.pdf. (11 February 2014).

Technology Law Development Group, 2003. Computer Output as Evidence Singapore Academy of Law. Available from: http://lwb.lawnet.com.sg/legal/lgl/html/freeaccess/tldgp/Computer_Output_as_Evidence.pdf. (24 December 2014).

Texas Explorer's Guide to Law Enforcement Training, 2012. Available from http://www.tleeaa.org/uploads/TLEEAA_Training_Guide.pdf. (22 October 2013).

Thomas, D. S, & Forcht, K. A. 2004. Legal methods of using computer forensics techniques for computer crime analysis and investigations, Volume 2 of 2004, James Madison University press. Available from: http://iacis.org/iis/2004/ThomasForcht.pdf. (03 April 2014).

Thomson, L.L. 2011. Admissibility of electronic documentation as evidence in U. S. court: The changing digital evidence landscape. Available from: http://www.crl.edu/sites/default/files/attachments/pages/Thomson-E-evidence-report.pdf. (04 January 2014).

Thomson, L. L. 2013, New challenges for admissibility of electronic evidence. Published in The SciTech Lawyer, Volume 9, Number 3. Available from:http://www.americanbar.org/content/dam/aba/events/science_technology/mobiledevices_new_challenges_admissibility_of_electronic_device.authcheckdam.pdf. (30 September 2013).

Tibasana, L. M. 2001. Effective administration of the police and prosecution in criminal justice: the practice and experience of the united republic of Tanzania. Available from: http://www.unafei.or.jp/english/pdf/RS_No60/No60_19PA_Tibasana.pdf. (22 November 2013).

Trepel, S. 2007. Digital Searches, General Warrants, and the case for the courts. Available from: http://yjolt.research.yale.edu/files/trepel-10-YJOLT-120.pdf. (22 November 2013).

Tubake, M. 2013. Cyber Crimes: *An Overview Online International Interdisciplinary Research Journal*, Volume-III, Issue-II, Karnataka State Law University Press, Hubli, India. Available from: http://www.oiirj.org/oiirj/mar-apr2013/18.pdf. (02 November 2013).

United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna, 2000. Available from: http://www.uncjin.org/Documents/congr10/10e.pdf. (12 October 2013).

United Nations Manual on the prevention and control of computer-related, 1999. Crime International review of criminal policy Nos. 43 and 44. Available from: http://www.uncjin.org/Documents/irpc4344.pdf. (12 January 2014).

United Nations Office on Drugs and Crime, 2005. The Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, Thailand Available from: http://www.unodc.org/unodc/en/crime-congress/crime-congresses-11-documents.html. (25 January, 2014).

United Nations Office on Drugs and Crime, 2013. Comprehensive Study on Cybercrime. Available from: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. (20 February 2014).

USA patriot Act of 2001. Available from: http://www.justice.gov/archive/ll/highlights.htm. (22 January 2014).

United States Department of Justice Search and Seizure Manual, 2002. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, United States Department of Justice. Available from: http://www.finer-bering.com/GULAW_PDFs/s&smanual2002.pdf. (20 November 2013).

Van As, M.V. & Van Schalkwyk, M.V. 2000. *Research and Information Management IV and Research Methodology*. First Edition. Florida: Technikon, SA.

Vella, P. 2013. Understanding Computer Evidence; Evidence Matters. Available from: http://www.1gis.co.uk/img/evidence.pdf (13 December 2013).

Vidas, T. 2006. Cyber Forensics, the basics. Available from: http://www.certconf.org/presentations/2006/files/WD4.pdf. (25 February 2014).

Walker, C. 2005. Computer Forensics: Bringing the Evidence to Court. Available from: http://www.infosecwriters.com/text_resources/pdf/Computer_Forensics_to_Court.pdf. (18 February 2014).

Wall, C. & Paroff, J. 2004. Cracking the Computer Forensics Mystery. Available from: https://www.krollontrack.com/publications/utahbarjournal.pdf. (11 September 2013).

Wang, M. 2008. Electronic evidence in China. Digital Evidence and Electronic Signature Law Review, Vol 5. Available from: http://sas-space.sas.ac.uk/5576/1/1822-2509-1-SM.pdf. (23 September 2013).

Watney, M. 2009. Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position", *Journal of Information, Law & Technology* (JILT). Available from: http://go.warwick.ac.uk/jilt/2009_1/Watney. (23 December 2013).

Welch, T. 1997. Computer Crime Investigation & Computer Forensics: Information Systems Security, Summer 97, Vol. 6 Issue 2, p56, 25p. Available from: http://ivneetsingh.blogspot.com/2012/07/computer-crime-investigation-computer.html. (02 April 2013).

Welch, T. 2012. *Computer Crime Investigation & Computer Forensics*: Information Systems Security, Summer 97, Vol. 6 Issue 2, p56, 25p. Available from: http://ivneetsingh.blogspot.com/2012/07/computer-crime-investigation-computer.html#!/2012/07/computer-crime-investigation-computer.html. (21 May 2013).

Welman, J. C, Kruger, S. J, & Mitchell, B 2005. *Research Methodology*. 3rd Ed. Cape Town: Oxford University Press, Oxford.

Welty, J. 2011. Warrant Searches of Computers, UNC school of Government. Available from: http://www.ncids.org/Defender%20Training/2011SpringConference/WarrantSearchesComputers.pdf (20 October 2013).

Whitley, R. & Figarelli, D. 2009. A simplified guide to evidence. National Forensic Science Technology Centre (NFSTC) Florida. Available from: http://www.crime-scene-investigator.net/SimplifiedGuideDigitalEvidence.pdf. (20 November 2013).

Wilkinson, S. 2010. Good practice guide for Computer –Electronic evidence, Association of Chief police Officers Guidelines, England, Wales and Ireland. Available from: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf. (24 March 2014).

Williams, Q. P. M. 2011. ACPO Good Practice Guide for Digital Evidence. Available from: http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf. (09 April 2013).

Winick, R. 1994 Searches and seizures of computers and computer data, Volume 8, number 1.Available from:

http://jolt.law.harvard.edu/articles/pdf/v08/08HarvJLTech075.pdf. (30 September 2013).

Witter, F. 2001. Legal Aspects of Collecting and Preserving Computer Forensic Evidence. Available from: http://www.giac.org/paper/gsec/636/legal-aspects-collecting-preserving-computer-forensic-evidence/101482. (25 December 2013).

Wori, O. 2014. Computer Crimes: Factors of Cybercriminal Activities Cloud Publications. *International Journal of Advanced Computer Science and Information Technology*. Volume 3, Issue 1, pp. 51-67 Wayne State University, Detroit press, USA. Available from: http://technical.cloud-journals.com/index.php/IJACSIT/article/view/Tech-136 (01 April 2014).

Yusoff, Y., Ismail, R. & Hassan, Z. 2011. Common phases of computer forensics Investigation models. *International Journal of Computer Science & Information Technology (IJCSIT*), Vol 3, No 3, University Tenaga National Press, Selangor, Malaysia. Available from: http://airccse.org/journal/jcsit/0611csit02.pdf (23 November 2013).

Zimbabwe. 2013. Constitution of Zimbabwe Amendment Act, no 1 of 2013: Printflow Private Limited.

Zimbabwe. 2004. Criminal law [codification and reform] Chapter 9:2 Act 23. Harare: Printflow Private Limited.

Zimbabwe. 2004. Criminal Procedure and Evidence (Chapter 9:07) Act, 14. Harare: Printflow Private Limited.

Zimbabwe Herald. 2009. Comment: "Promoting Global Cyber security", 11 December: 2009.

Zimbabwe. 1998. Private Investigators and Security Guards (Control) Act 8. Harare: Printflow Private Limited.

Zimbabwe.2001. Zimbabwe Republic Police (Chapter 11:10) Act 22. Harare: Printflow Private limited.

Zimbabwe. 2013. Zimbabwe Serious Offences (Confiscation of Profits) Act (*Chapter 9:17*). Harare: Printflow Private Limited.

LIST OF CASES

A.G. (Nova Scotia) v. Macintyre, 1982. 1 S.C.R.

Associated Newspapers of Zimbabwe (Pvt) Ltd v Madzingo NO & Anor, 2003. HH-157-03

Capital Radio (Pvt) Ltd v Minister of Information & Ors (2), 2000. (2) ZLR 265 (H),

Chizano v Commissioner of Police, 1988. HH-392-88;

Daubert vs. Merrell Dow Pharmaceuticals, 1993. (92-102), 509 U.S. 579

Elliot v. Commissioner of Police, 1986. (1) ZLR 228 (H

Frye v. United States, 1923. 54 App. D.C. 46, 47, 293 F. 1013, 1014

Guest v. Leis, 2001. 255 F. 3d 325 - Court of Appeals, 6th Circuit

Kennedy v. Los Angeles Police Department, 1989 by Ninth California Court of Appeals (901 Federal Second pp. 702–716)

Kyllo v. United States, 2001. 533 U.S.27, 121 S.Ct. 2038.

Paradza v Chirwa and others, 2005. (2) ZLR 94 (S),

S v Bennet, 2009. (CRB 178/09) 2010. ZWHHC 79,

S v Mutemi, 1998. (2) ZLR 290 (HC

S v Ndebele and another, 2011. (SS16/2010) ZAGPJHC 41; 2012 (1) SACR 245 (GSJ)

ANNEXURE "A"

SAMPLE A
INTERVIEW SCHEDULE

INVESTIGATORS

TOPIC: PROCEDURES FOR SEARCHING EVIDENCE IN THE INVESTIGATION OF COMPUTER RELATED CRIME IN BULAWAYO, ZIMBABWE.

RESEARCH AIM

Therefore, the aim of this research is to determine the procedures that need to be followed when searching for evidence during investigation of computer related crimes with the intention to improve admissibility of such evidence.

RESEARCH QUESTIONS

This research seeks to address the following questions;

- What does computer related crime entail?
- How are searching procedures executed during investigation of computer related crime for evidence to be admissible in court?

You are kindly requested to answer the following questions in this interview schedule for the researcher. The information you provide will be used in a research project for a Master of Technology degree in Forensic Investigation registered with the University of South Africa.

You don't not need to identify yourself and, similar, the researcher will uphold anonymity in that there will be no possibility of any participants being identified or linked in any way in the research findings in the final research report. Participating in the study is voluntary and participants may withdraw from the study at any stage. The questionnaire is not time restricted and you may consider your responses carefully. Normally half an hour would be sufficient.

Your answers will be noted by the interviewer on paper and kindly seek clarification where required.

Lastly note that the analysed data will be published in a research report. Written permission has been obtained from the Commissioner General of Police in advance for the interview to be conducted.

I hereby give permission to be interviewed and that information supplied by me can be used in this research

Yes / No

A. Historical Information

1. Are you involved in the investigation of crime?

Yes / No

2. How long have you been an investigator?

1 – 5 years 5 -10 years 10 -15 years

3. Have you undergone basic detective training?

Yes / No

4. Did you receive any training related to the investigation computer related crimes?

Yes / No

B. Computer-related crime

1. What do you understand under the concept “computer crime”?
2. What do you understand by the term “computer forensics”?
3. Name and describe different types of crime scene?
4. As an investigator, what rights mandates you to investigate crime?
5. What qualities should investigator have in order to investigate computer related crimes?
6. What are the responsibilities of investigator during the investigation of crime?
7. What is objectives investigation?

8. What is the purpose of investigation?

9. Name and describe the different types of evidence?
10. What types of evidence is found at the computer related crime?
11. Where does computer related crime resort under traditional crimes?
12. Explain the main ways in which computer can be used in crime?
13. What is classification of computer related crime?
14. Briefly explain how will you approach computer crime scene?
15. What are investigation models developed by computing experts?

C. The procedures for searching evidence in computer related crimes

16. Define the concept “search”?
17. Name software tools that can be used in searching evidence during the investigation of computer crime?
18. What are the standards or legal requirements for searching and preserving computer evidence?
19. According to your knowledge, are traditional searching procedures applicable to physical objects also apply to the intangible objects?
20. In terms of your experience, what are basic strategies and procedures for searching computer evidence?
21. .Can information that has been retrieved through software tool be accepted as evidence during trial
22. Why is important to maintain chain of custody when collecting and preserving computer crime evidence?
23. Why should computer forensic expert be used to search and preserve computer evidence?
24. .What are the legal requirements for the admissibility of computer evidence in court?
25. How should computer evidence be presented in court?
26. What are the challenges faced by investigators in dealing with computer evidence?

ANNEXURE "B"

SAMPLE B

INTERVIEW SCHEDULE

POLICE PUBLIC PROSECUTORS

TOPIC: PROCEDURES FOR SEARCHING EVIDENCE IN THE INVESTIGATION OF COMPUTER RELATED CRIME IN BULAWAYO, ZIMBABWE.

RESEARCH AIM

Therefore, the aim of this research is to determine the procedures that need to be followed when searching for evidence during investigation of computer related crimes with the intention to improve admissibility of such evidence.

RESEARCH QUESTIONS

This research seeks to address the following questions;

- What does computer related crime entail?
- How are searching procedures executed during investigation of computer related crime for evidence to be admissible in court?

You are kindly requested to answer the following questions in this interview schedule for the researcher. The information you provide will be used in a research project for a Master of Technology degree in Forensic Investigation registered with the University of South Africa.

You don't need to identify yourself and, similar, the researcher will uphold anonymity in that there will be no possibility of any participants being identified or linked in any way in the research findings in the final research report. Participating in the study is voluntary and participants may withdraw from the study at any stage. The questionnaire is not time

restricted and you may consider your responses carefully. Normally half an hour would be sufficient.

Your answers will be noted by the interviewer on paper and kindly seek clarification where required.

Lastly, note that that the analysed data will be published in a research report. Written permission has been obtained from the Commissioner General of Police in advance for the interview to be conducted.

I hereby give permission to be interviewed and that information supplied by me can be used in this research

Yes / No

A. Historical Information

1. Are you involved in the investigation of crime?

Yes / No

2. How long have you been an investigator?

1 – 5 years 5 -10 years 10 -15 years

3. Have you undergone basic detective training?

Yes / No

4. Did you receive any training related to the investigation of computer related crimes?

Yes / No

B. Computer-related crime

1. What do you understand under the concept “computer crime”?
2. What do you understand by the term “computer forensics”?
3. Name and describe different types of evidence?
4. What types of evidence is found at the computer related crime?
5. Where does computer related crime resort under traditional crimes?
6. What is the different between computer evidence and document evidence?

7. Define the concept “search”
8. Name software tools that can be used in searching evidence during the investigation of computer crime?
9. What are the standards or legal requirements for searching and preserving computer evidence?
10. In terms of your experience, what are basic strategies and procedures for searching computer evidence?
11. Can information that has been retrieved through software tool be used as evidence during trial?
12. Why is important to maintain chain of custody when searching and preserving computer crime evidence?
13. Why should computer forensic expert be used to search and preserve computer evidence?
14. What are the legal requirements for the admissibility of computer evidence in court?
15. What are the challenges faced by Police Public Prosecutors in dealing with computer evidence?

ANNEXURE "C"

ZIMBABWE REPUBLIC POLICE

Official Communications should not be addressed to individuals

Telegrams 'COMPOL':

Telephone HARARE 700171

GENERAL HEADQUARTERS, HARARE

corner 7th St./Josiah Chinamano Avenue

P.O. Box CY 34, CAUSEWAY

Telex: 24328 (ZRPHQ): Fax: (263)-(4)-7267 ZIMBABWE.

12 September 2013

MBCA Bank Limited
74 Main Street
BULAWAYO

Attention: **Mr Njabulo Ncube**

APPLICATION FOR PERMISSION TO CARRY OUT A RESEARCH WITHIN THE ORGANISATION: YOURSELF

Reference is made to your letter dated 15 July 2013 in connection with the above subject.

Please be kindly advised that your application to carry out a research within the Zimbabwe Republic Police was approved.

You may wish to liaise with Officer Commanding Police, Bulawayo Province on 09 60146 for implementation modalities.

Referred for your information, please.

[**JC CHENGETA**] Senior Assistant Commissioner
Chief Staff Officer [**Human Resources**]
to the **COMMISSIONER GENERAL OF POLICE**

ANNEXURE "D"

ZIMBABWE REPUBLIC POLICE

Official Communication
Should not be addressed to
individuals

Bulawayo Provincial Headquarters.,
P.O.Box 701.
Bulawayo
Zimbabwe.

Telegrams:Propol Telephone Bulawayo: 60146: Telex: 72220 : Fax: (263)-(09)-72220

REF: .....

5th February 2014

The University of South Africa [UNISA]
COLLEGE OF LAW

RE: PROCEDURE FOR SEARCHING EVIDENCE IN THE INVESTIGATION OF COMPUTER RELATED CRIME AT BULAWAYO; UNIVERSITY OF SOUTH AFRICA [UNISA]: NJABULO NCUBE STUDENT 46874774

This serves to confirm that in the Zimbabwe Republic Police there are certain Police Officers with requisite qualifications to prosecute who are seconded for prosecution duties under the Prosecutor General. These Officers however, remain subject to the Command of the Zimbabwe Republic Police.

[S. MUTAMBA] Senior Assistant Commissioner
Officer Commanding Police
BULAWAYO PROVINCE

HEADQUARTERS
ZIMBABWE REPUBLIC POLICE
OFFICER COMMANDING
06 FEB 2014
BULAWAYO PROVINCE
P.O. BOX 701 BULAWAYO
TEL: 09-65763 / 60146

/tsn.

c.c. NJABULO NCUBE
2058 Mahatshula North
BULAWAYO

1. Your minute dated 5th February 2014 is relevant.
2. For your information.

ANNEXURE "E"

ZIMBABWE OPEN UNIVERSITY
"Empowerment Through Open Learning" ®
FACULTY OF ARTS AND EDUCATION
DEPARTMENT OF LANGUAGES AND LITERATURE

No. 44 Anchor House
Cnr Fort St & 12th Avenue
Bulawayo
Zimbabwe
+263-884054/55

24 June 2015

To Whom It May Concern

RE: EDITING/PROOFREADING CONFIRMATION FOR NJABULO NCUBE DISSERTATION (STUDENT NUMBER: 46874674)

This note serves to confirm that the Magister Technologiae dissertation by the above mentioned candidate, titled *'Procedures for searching evidence in the investigation of computer-related crime in Bulawayo, Zimbabwe'* in the subject Forensic Investigation for submission to the University of South Africa, was edited/ proofread in the Department and recommendations made. The effecting of the recommendations remained exclusively with the candidate at the finalisation of the document.

Thank you

N. Sibanda

Nhlanhla Sibanda (Mr)
(Lecturer- English & Communication Studies)
(MA English; MSc Peace, Leadership & Conflict Resolution; BA (Hons) English; Dip. Ed; Dip in Ministry)