

**A SURVEY OF COMPUTER FORENSICS PRACTICES IN  
LITIGATION SUPPORT: THE CASE OF THE BANKING  
INDUSTRY IN KENYA**

**BY**

**NGEMU, ANNEROSE  
D/61/P/7914/00**

UNIVERSITY OF NAIROBI LIBRARY



0282372 2

**A MANAGEMENT RESEARCH PROJECT SUBMITTED IN  
PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE  
AWARD OF MASTER OF BUSINESS ADMINISTRATION (MBA)  
DEGREE, FACULTY OF COMMERCE, UNIVERSITY OF  
NAIROBI**

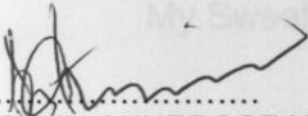
**MARCH, 2005**

## DECLARATION

THIS MANAGEMENT RESEARCH PROJECT IS MY ORIGINAL WORK AND HAS NOT BEEN PRESENTED FOR A DEGREE IN ANY OTHER UNIVERSITY

SIGNED

DATE

  
.....

12/10/2005  
.....

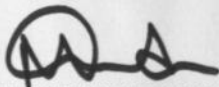
NGEMU ANNEROSE NDOTI

To my Husband, John N. Nguni,  
My Sweet toddlers, Sharon M. Nguni, Claire M. Nguni  
&  
Other family members  
For their understanding, support and encouragement  
throughout the course.

THIS MANAGEMENT RESEARCH PROJECT HAS BEEN SUBMITTED FOR EXAMINATION WITH MY APPROVAL AS THE UNIVERSITY SUPERVISOR

SIGNED

DATE

  
.....

13/10/2005  
.....

NIXON MUGANDA  
LECTURER, DEPARTMENT OF MANAGEMENT SCIENCE  
FACULTY OF COMMERCE  
UNIVERSITY OF NAIROBI

MARCH, 2005

## ACKNOWLEDGEMENTS

I wish to extend my sincere thanks to several people who directly or indirectly contributed to my successful completion of the MBA Course.

First and foremost, I wish to thank my family for the full support through out the course. Special gratitude goes to my husband for being so understanding, supportive and encouraging during the course period. To my Sister Consolata Muriu for taking very good care of my little baby to enable me to complete the course.

### DEDICATION

To my Husband, John N. Nguni,  
My Sweet toddlers, Sharon M. Nguni; Claire M. Nguni  
&  
Other family members

Special thanks go to my supervisor, Wilson Mwangi for his invaluable comments, patience and guidance throughout the course.

I also wish to thank my friends, namely, Mrs. Nthenge, Josephine Towett and Alice Kisi for their encouragement and support throughout the project period.

Last but not least, I thank all the respondents who enabled me to collect the data.

Above all, I thank God Almighty for everything.

## ACKNOWLEDGEMENTS

I wish to extend my sincere thanks to several people who directly or indirectly contributed to my successful completion of the MBA Course.

First and foremost, I wish to thank my family for the full support through out the course. Special gratitude goes to my husband for being so understanding, supportive and encouraging during the course period. To my Sister Consolata Mueni for taking very good care of my little baby to enable me resume classes immediately after her arrival.

Special thanks also go to my supervisor, Nixon Muganda for his invaluable comments, patience and guidance through this project.

I also wish to thank my friends, namely, Mrs. Nthenge, Josephine Towett and Alice Kiai for their encouragement and support throughout the project period.

Last but not least, I thank all the respondents who enabled me to collect the data.

Above all, I thank **God Almighty** for everything.

- i.) Identification & collection of evidence as well as the forms of production for computer evidence;
- ii.) On-site inspection of information systems and related costs;
- iii.) Access to computer forensics guidelines to guide the computer forensics investigations process methodology;
- iv.) Analysis & presentation of computer evidence, and
- v.) Access to expert assistance for provision of assistance in the handling and presentation of computer evidence.

## **ABSTRACT**

Computer Forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information. With the proliferation of computers in day-to-day operations as well as several technology driven initiatives such as the E-commerce initiative, there has been an increase in criminal activities by use of computers or even through the web. Computer forensics, therefore, aims at collecting evidence from computer systems and computer media that can be preserved and analyzed by the investigator and presented in court to aid in prosecution of criminals. In this process, there are many complexities that must be considered and the investigator must always be able to justify their actions.

The aim of the study was to investigate the existence of computer evidence; assess the extent of adoption of computer forensics practices and identify the challenges faced by the banking industry in Kenya when collecting and using computer evidence for litigation support. A census survey of the Banking Industry was conducted. Data analysis was done using descriptive statistics and factor analysis.

According to the findings of the survey, various computer forensic practices have been largely adopted in litigation support within the Kenyan Banking industry. The most adopted practices were identified as: - Determination of legal right; Gathering of evidence; Analysis of gathered evidence; Correlation of evidence to events that occurred and Backup procedures

Additionally, the main challenges that banks encounter in collecting and using forensic evidence for litigation support were identified as: -

- i.) Identification & collection of evidence as well as the forms of production for computer evidence;
- ii.) On-site inspection of information systems and related costs;
- iii.) Access to computer forensics guidelines to guide the computer forensics investigations process methodology;
- iv.) Analysis & presentation of computer evidence; and
- v.) Access to expert assistance for provision of assistance in the handling and presentation of computer evidence.

## LIST OF CHARTS

## LIST OF TABLES

Table 1: Cyber-Crime in Singapore .....	4
Table 2: Computer Forensic Analytical Methods .....	22
Table 3: Customer Base .....	31
Table 4: Transaction Authorization Methods .....	34
Table 5: Types of Fraud .....	35
Table 6: How frauds were discovered .....	36
Table 7: Type of Computer evidence.....	37
Table 8: Extent to which evidence gathering practices/procedures are used .....	38
Table 9: Challenges attached to activities in computer forensic investigations ..	40
Table 10: Total Variance Explained.....	43
Table 11: Pattern Matrix 1 .....	44
Table 12: Total Variance Explained.....	47
Table 13: Pattern Matrix 1 .....	48

## **LIST OF CHARTS**

Chart 1: Bank Ownership .....	30
Chart 2: Number of Branches .....	31
Chart 3: Level of IT in the Banks .....	32
Chart 4: Link of Branches to the Central Server .....	33
Chart 5: Number of staff connected to a Central Server .....	33
Chart 6: Top five frauds .....	35
Chart 7: Retrieval of Computer evidence.....	37

# LIST OF DIAGRAMS

Diagram 1: Computer Forensic Science Investigation Process ..... 14

CHAPTER ONE: INTRODUCTION .....	2
1.1. Background to the Study .....	2
1.2. Statement of the Problem .....	6
1.3. Objectives of the study .....	7
1.4. Importance of study .....	8
CHAPTER TWO: LITERATURE REVIEW .....	9
2.1. Introduction .....	9
2.1.1. COMPUTER FORENSICS .....	9
2.2. The Incident Response Plan .....	11
2.3. Computer Forensic Science: The Investigation Process .....	12
2.3.1. ELECTRONIC TYPES OF DATA .....	13
2.3.2. COMPUTER FORENSICS PROCESS METHODOLOGY .....	14
2.4. Unique Challenges of Computer-Based Discovery .....	22
2.4.1. PRESERVATION OF DATA .....	22
2.4.2. LOCATION AND VOLUME OF DATA .....	22
2.4.3. E-MAIL AS A UNIQUE PHENOMENON .....	23
2.4.4. DELETED DOCUMENTS .....	24
2.4.5. BACKUP TAPES .....	24
2.4.6. ARCHIVES AND LEGACY DATA .....	24
2.4.7. ON-SITE INSPECTION .....	25
2.4.8. FORM OF PRODUCTION .....	25
2.4.9. NEED FOR EXPERT ASSISTANCE .....	26
2.5. Overview of the Banking sector .....	26
2.6. Conclusion .....	27
CHAPTER THREE: RESEARCH METHODOLOGY .....	28
3.1. Research Design .....	28
3.2. The population .....	28
3.3. Data Description and Collection .....	28
3.4. Data Analysis .....	28



# TABLE OF CONTENTS

<b>CHAPTER ONE: INTRODUCTION</b> .....	<b>2</b>
1.1. Background to the Study .....	2
1.2. Statement of the Problem.....	6
1.3. Objectives of the study .....	7
1.4. Importance of study .....	8
<b>CHAPTER TWO: LITERATURE REVIEW</b> .....	<b>9</b>
2.1. Introduction.....	9
2.1.1. COMPUTER FORENSICS .....	9
2.2. The Incident Response Plan.....	11
2.3. Computer Forensic Science: The Investigation Process .....	12
2.3.1. ELECTRONIC TYPES OF DATA .....	13
2.3.2. COMPUTER FORENSICS PROCESS METHODOLOGY .....	14
2.4. Unique Challenges of Computer-Based Discovery.....	22
2.4.1. PRESERVATION OF DATA .....	22
2.4.2. LOCATION AND VOLUME OF DATA .....	22
2.4.3. E-MAIL AS A UNIQUE PHENOMENON .....	23
2.4.4. DELETED DOCUMENTS .....	24
2.4.5. BACKUP TAPES.....	24
2.4.6. ARCHIVES AND LEGACY DATA .....	24
2.4.7. ON-SITE INSPECTION .....	25
2.4.8. FORM OF PRODUCTION .....	25
2.4.9. NEED FOR EXPERT ASSISTANCE.....	26
2.5. Overview of the Banking sector .....	26
2.6. Conclusion .....	27
<b>CHAPTER THREE: RESEARCH METHODOLOGY</b> .....	<b>28</b>
3.1. Research Design .....	28
3.2. The population .....	28
3.3. Data Description and Collection.....	28
3.4. Data Analysis.....	28

<b>CHAPTER FOUR: DATA ANALYSIS &amp; FINDINGS .....</b>	<b>30</b>
4.1. Introduction.....	30
4.2. Bank demographic information.....	30
4.2.1. RESPONSE RATE .....	30
4.2.2. OWNERSHIP OF BANKS .....	30
4.2.3. CUSTOMER BASE .....	31
4.2.4. NUMBER OF BRANCHES .....	31
4.3. Use of Information Technology in the Banks .....	32
4.3.1. LEVEL OF INFORMATION TECHNOLOGY USE .....	32
4.3.2. LINK OF BRANCHES TO A CENTRAL SERVER .....	32
4.3.3. MEMBERS OF STAFF CAN CURRENTLY CONNECT TO THE CENTRAL SERVER.....	33
4.4. Existence of Computer Forensics .....	34
4.4.1. TRANSACTION AUTHORIZATION METHOD.....	34
4.4.2. FRAUDS.....	34
4.4.3. HOW FRAUDS WERE DISCOVERED.....	36
4.5. Computer forensics practices.....	36
4.5.1. RETRIEVAL OF COMPUTER EVIDENCE TO SUPPORT LITIGATION .....	36
4.5.2. TYPE OF COMPUTER EVIDENCE RETRIEVED TO SUPPORT LITIGATION.....	37
4.5.3. EXTENT TO WHICH THE VARIOUS EVIDENCE GATHERING PRACTICES/PROCEDURES ARE UTILIZED. ....	37
4.6. Challenges of Computer Forensics.....	40
4.6.1. LEVEL OF CHALLENGES ATTACHED TO ACTIVITIES CARRIED OUT IN COMPUTER FORENSICS INVESTIGATION. ....	40
4.7. Section II- Factor Analysis .....	42
4.7.1.....EXTENT TO WHICH THE BANK PRACTICED THE LISTED PROCEDURES WHEN GATHERING EVIDENCE.....	42
4.7.2. LEVEL OF CHALLENGES ATTACHED TO ACTIVITIES CARRIED OUT IN COMPUTER FORENSICS INVESTIGATION. ....	47
<b>CHAPTER FIVE: SUMMARY AND CONCLUSIONS.....</b>	<b>51</b>
5.1. Introduction.....	51
5.2. Discussions .....	51
5.2.1. EXISTENCE OF COMPUTER FORENSICS .....	51

5.2.2.	SUMMARY DISCUSSIONS IN LIGHT OF THE STUDY OBJECTIVES.....	52
5.2.3.	FACTOR ANALYSIS DISCUSSIONS.....	55
5.3.	Conclusions.....	60
5.4.	Limitations of the Study & Suggestions for Further Research .....	61
5.4.1.	LIMITATIONS .....	61
5.4.2.	SUGGESTIONS FOR FURTHER RESEARCH .....	62
<b>REFERENCES</b>	.....	<b>63</b>
<b>APPENDICES</b>	.....	<b>66</b>
Appendix 1:	Letter of Introduction .....	66
Appendix 2:	Questionnaire .....	67
Appendix 3:	List of the Respondent Banks .....	73

warehouses to store their continuously growing data bank (Oswies, 2001).

here in Kenya, most organizations whether business entities, agencies of the government or other institutions have for an extended period of time relied on computerized systems in managing their operations. These systems have been applied in daily operations for a variety of uses. The roles range from support of standard office administration tasks (document production via word processing, messaging via e-mail, communicating within and outside the organization, staff scheduling, variety of personal and organizational productivity tools etc.); through financial administration (accounting), and increasingly their application especially in the Banking sector has extended to critical core business operations. Typically these are processes within the scope transaction processing, management, product design, customer and vendor/relationship management as well as communication.

The banking industry in Kenya for instance, has become highly dependant on Information Systems or would not even exist, certainly in its current form, unless these computerized resources were available. In the course of utilizing the various electronic tools, Banks have generated and accumulated vast amounts of data and documents. Following sound business practices, they have exercised due care to backup their data files in the most practicable format available at the time, typically on a variety of magnetic and optical media. Despite the fast pace of technological evolution, Banks have aggressively invested in the newest technologies, possibly out of competitive and strategic prerogatives. As such the various computerized forms of data and documents have continued to be an endless challenge increasing in complexity almost daily when for instance many technologies, very popular in their day have completely

# CHAPTER ONE: INTRODUCTION

## 1.1. Background to the Study

Over the last decade or more, there has been much discussion in our world about the threats to information security particularly from criminal and terrorist cyber-attacks (Sarah; 2001). Criminals are becoming more sophisticated in committing crimes as computers continue to be encountered in almost every type of criminal activity (Purdy; 1993). However, as computer technology advances, businesses are increasingly utilizing these technological advancements to improve their business operations and market potential. Increasingly, consumers in Kenya like other parts of the world can now pay bills online; order anything from books to groceries to automobile tires online, they can even try on clothing. Internally, businesses use such technological tools as wireless links, Local Area Networks, Wide Area Networks, and palm pilots to share data and information, Net meetings to coordinate project efforts, and data warehouses to store their continuously growing data bank (Oseles, 2001).

Here in Kenya, most organizations whether business entities, agencies of the government or civic institutions have for an extended period of time relied on computerized systems in managing their operations. These systems have been applied in daily operations for a variety of roles. The roles range from support of standard office administration tasks (document production via word processing, messaging via e-mail, communicating within and outside the organization, staff scheduling, variety of personal and organizational productivity tools etc.), through financial administration (accounting), and increasingly their application especially in the Banking sector has extended to critical, core business operations. Typically these are processes within the actual transaction processing, management, product design, customer and vendor relationship management as well as communication.

The banking industry in Kenya for instance, has become highly dependant on Information Systems or would not even exist, certainly in its current form, unless these computerized resources were available. In the course of utilizing the various electronic tools, Banks have generated and accumulated vast amounts of data and documents. Following sound business practices, they have exercised due care to backup their data files in the most practicable format available at the time, typically on a variety of magnetic and optical media. Despite the fast pace of technological evolution, Banks have aggressively invested in the newest technologies, possibly out of competitive and strategic prerogatives. As such the various computerized forms of data and documents have continued to be an endless challenge increasing in complexity almost daily when for instance many technologies, very popular in their day have completely

disappeared from the marketplace, even as the data created using them continues to be stored/preserved.

With this vast amount of important and sensitive data flowing around, it is readily available to fall into unintended or malicious hands. Given the increased usage of computer technology, computer crime is likely to be on the rise, as electronic data is frequently accessed for unintended purposes. Electronic data in this case can include "any record, file, source code, program, computer manufacturer specifications, and other information imprinted on a computer storage device" (The Center for Computer Forensics 2000).

Purdy (1993) argues that information stored in computers and other electronic media has become the target of criminal activity. Information such as social security and credit card numbers, intellectual property, proprietary information, contract information, classified documents, etc., has been targeted. Further, the threat of malicious destruction of software, employee sabotage, identity theft, blackmail, sexual harassment, and commercial and government espionage is on the rise.

Else where, according to a Cyber crime and Information Security Survey report (Country Report on Singapore) done within Singapore in 2002, it was noted, "As the use of Information Communication & Technology becomes more pervasive in society, an increasing trend in the perpetration of technology related crimes could be expected". This is further validated by the given statistics taken from Singapore during the survey:

**Table 1: Cyber-crime in Singapore**

Offence	Number Of Cases				
	1997	1998	1999	2000	2001
Hacking	3	5	13	9	15
Access to commit a Further Offence (Computer Fraud)	4	2	3	1	4
Unauthorized Use of Computer Service	20	101	159	157	52
Other Offences	12	8	10	24	66
Total	39	116	185	191	137

**Source: - INFOCOMM security, Country Report on Singapore November 2002.**

While the figures may appear low, the consequences of computer crimes is markedly higher than the traditional crimes not involving electronic data as indicated by a 1999 Computer Security Institute (CSI)/FBI survey. According to the survey results, an average bank robbery netted \$2,500 while the average computer crime netted \$500,000 (Armstrong 2001). In addition to this, the Internet has made targets much more accessible and the risks involved for the criminal much lower than with traditional crimes. The trend exhibited by the statistics over the years was unwavering. Accordingly therefore, there is a need to arrest the trend of increasing information and communications technology related offences quickly and through a multiple-pronged approach, especially as the Internet finds itself into more and more aspects of life in the ensuing years.

Elsewhere in the US, according to a Federal Bureau of Investigation (FBI) report (2001), in the year 2000 there were 2,032 cases opened involving cyber crime. In Australia, a survey report on Computer crime and security (2002) revealed that 67% of the respondents experienced a harmful computer security incident, which harmed the confidentiality, integrity and availability of network data or systems. Right here in Kenya, as Information Communication & Technology (ICT) investment and utilization continue to grow tremendously a similar trend has been observed. Like other sectors worldwide; Banks all over the world are exposed to cyber criminals and Kenya is no exception. Former Police Commissioner Mr. Nyaseda speaking during the fourth meeting of the Interpol African Working Party on Information Technology Crime workshop in Nairobi (February, 2004) noted that, Fraudsters apply various methods and ways to swindle owners of bank accounts and credit cards. He further noted that though some of the frauds have gone without being reported, experts have estimated the losses run into millions of Kenyan shillings," Nyaseda said: "I have noted with concern the ever-increasing 4-1-9 type of frauds in my country. The attacks on the banking sector by computer fraudsters have been devastating." Nyaseda further cited lack of trained security agents, the transient nature of computer data and the ever-evolving information technology world as some of the challenges facing cyber crime investigators.

Still on Information Systems compromise, the growth in Kenya's burgeoning credit card industry could be affected by a sharp increase in fraud cases on internationally- and locally issued credit cards, according to a report on "Credit Card Fraud: Kenya Losing Millions" published in East African Standard Monday, April 19, 2004. According to the report in the month of March 2004 alone, the Central Bank of Kenya reported about USD 128,000 to have been lost to fraud on international credit cards. The Fraud on locally issued cards was also on the rise, with the Kenya Police noting growth in "own-card" fraud, where Kenyans report their card to have been

lost or stolen on a weekend, before exceeding their card limit on Saturday and Sunday and reporting the loss to the card issuer on the Monday.

It is against the above background that Isner (2003) argues that, as a result of computer related crimes; criminals steal billions of dollars each year. He further notes that in today's digitally connected world, computers are rapidly becoming a vector for those criminals to carry out their crime. The Kenyan situation is not any different since many organizations; especially those in the financial services sector have undertaken computerization of their operations. There have been huge ICT investments (Nyambati, 2001; Njogu, 2004); and, therefore, the firms in this sector, just as in other parts of the world as reported in the other studies, need to be worried about the incidences of computer crime.

Purdy (1993) notes that, almost overnight, personal computers have changed the way the world does business and as a result they have changed the world's view of evidence because computers are used more and more as tools in the commission of 'traditional' crimes. Further Purdy (1993) argues that computer evidence has henceforth become a 'fact of life' for essentially all law enforcement agencies and many are just beginning to explore their options in dealing with this new venue. A similar view is shared in the On track Cyber Crime and Computer Forensics Newsletter (October 2003 issue) where technology based evidence is seen to continue playing a larger role in litigation and internal company investigations with lawyers and investigators expected to comprehend the inner workings of computers and how they relate to any computer conduct at issue.

Computer forensics practice, therefore, may be viewed as a necessity for those firms that depend on computerized operations, recognizing that any Information System is not 100% foolproof. As Villano (2001) says, "Once regarded by technophiles as an obscure component of network security, the discipline has blossomed into a science of its own". Forensics specialists can draw on an array of methods for discovering data that resides in a computer system or recovering deleted, encrypted, or damaged file information (Gilmore, 2001).

Important to note however, is the fact that, legal proof is what is demonstrated before the court, that which can be used at arriving at a conclusion from a specific set of circumstances. Although the reliability of forensically located and recovered data is like any other evidence, it must be: admissible, authentic, accurate, complete and convincing to juries (Sommer, 1997). According to Sommer, electronic evidence is in a way different from other evidence because computer data: can change from moment to moment within a computer and along a

transmission line, can be easily altered without trace and can be changed during evidence collection given that computers create evidence as well as record it. (March 26, 2003). In other

With Information and Communication technologies being key drivers behind economic and social progression, the relationship therefore between the "information society" and "legal society" becomes increasingly close. An increase in the number of cases which will employ computer evidence for their resolution as virtually all business information, is processed and stored electronically is expected to continue growing. The perceived "digital divide" between the legal and Information technology professionals will, therefore, become history.

## 1.2. Statement of the Problem

Worldwide, crimes associated with the theft of information, global terrorism and violence can now be conducted online (E-Commerce Security, 2001). As a relatively new scientific discipline, known as computer forensics, created in the mid-1990's to obtain computer evidence; its practice in Kenya has not been documented before largely due to the unavailability of prior research, and, much more importantly the lack of legislation with regard to computer crimes. Yet, evidently, many organizations, especially within the banking sector depend for their survival on computer processing (Nyambati, 2001). This lack of legislation specifically targeting computer crimes and other ICT related crimes poses a great risk to these organizations that spend millions of shillings each year on technology investments, yet there are increasing incidences of computer crimes as reported elsewhere.

Problems arise when crimes are committed from computer transactions for instance. Contacting the appropriate authorities initially can, according to Shipley (2001), "expedite...response to a crime scene for the easier..." a CEO "makes it for law enforcement, the faster a perpetrator will get arrested." If there is no way of tracing or even a law to expedite this, then the enormity of the problem is apparent. According to Gilmore (2001), "An ill-prepared Executive with no formal corporate policy or plan for facing computer hacks and security breaches places the company in jeopardy and risks the corporate assets that they have been hired to protect."

As noted earlier, while technology continues to drive enormous business in the Kenyan scene, there is no law in the Kenyan Constitution that governs its practice. Just like any part of the world though, computer crimes have and will continue to be committed in Kenya. Embezzlement, theft of trade secrets, abuse of the Internet and unauthorized use outside employment on company time are common occurrences in the workplace. In some cases,



computer hard disk drives have been reformatted in an attempt to hide the evidence as recently witnessed in the Euro Bank saga right here in Kenya (Daily Nation, March 26, 2003). In other cases, critical passwords are changed in an attempt to block access to the evidence. Though the lack of attention on laws governing cyber crimes are not only limited to our national scene, the lack of legislation implies that electronic evidence may remain largely un-addressed and therefore gray even when it has safely been found and preserved.

Further it is essential to note that one of the crucial aspects and also major challenges in electronic evidence is not only finding, but also preserving the data, as electronic evidence is fragile, and can easily be modified and deleted. The most common legal difficulty faced by organizations seeking to redress cyber-crime in the court is having digitally based evidence accepted. Gathering legal evidence goes beyond normal data recovery (Walker, 2001). Although such evidence may be authentic, reliable and complete it may not be in conformity with the existing common law and legislative rules.

Assuming that a law was enacted in parliament to regulate the ICT profession, there would still remain a challenge on the limited knowledge and experience that the lawyers who would be asking their clients for evidence have. It means that, a new breed of lawyers who mix ICT and Law practices would have to emerge. In their absence, expert witness could be called in or we would witness more injustice than justice done. Law enforcement agencies on the other hand will be under intense scrutiny on methodologies used to gather evidence. They will have to show that, no one could have made changes to the information contained on a computer system from where the evidence was collected.

The basis for this research project therefore hinges on these apparent gaps, with a view to first understanding the computer forensic practices with regard to the banking industry. It will investigate the existence, extent of adoption of computer forensics practices. Further, it will investigate the challenges faced by the banking industry in Kenya while producing evidence from Information Systems that will meet the rigors of court requirements in legal proceedings as well as in using the evidence for litigation.

### **1.3. Objectives of the study**

- 1) To determine the extent of adoption of computer forensics practices in litigation support within the banking industry in Kenya; and
- 2) To identify the challenges faced by the banking industry in Kenya while collecting and using computer evidence for litigation support.

## 1.4. Importance of study

The study will be significant to the banking industry, especially to Information Systems Audit Managers involved in gathering, preserving and presenting computer based evidence findings in litigation support. It will highlight the challenges faced by the banking industry when identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in Kenya and ways of mitigating the challenges. To other sectors of the economy, it will provide a start to finish account for what informed CEO's should consider when instituting electronic evidence collection after an Information Systems compromise as they realize that today there is a 70% chance that their company will become part of the growing statistic of business affected and impacted by computer-based crimes.

Additionally as the Kenyan nation becomes more and more technologically advanced; it also becomes further technologically dependent. Fighting cyber crime, therefore, will require a coordinated approach, which unites computer forensics and law enforcement agencies in their effort to helping the state and law enforcement meet the challenges of the 21st century in as far as cyber crimes are concerned. The findings of the research will therefore contribute in any nationwide initiatives aimed at the formulation of a national plan, which ensures that staffing; equipment, and training resources are maximized for the fighting of cyber crime.

Given that the country will continue solving cyber-crimes there is increasing need for qualified computer forensic specialists. The results of the study will also be of assistance during the formulation and drawing of new training material and university programs in the area of Computer forensic science. Finally, the research findings will be of value to other researchers as a basis for further research especially in widening the research to cover all sectors of the economy, as this was limited to banking sector only.

To other researchers, it will be useful for further research as this study only focuses on the banking industry. They could use the findings of this research to expand to other sectors of the economy not looked at during this study.

# CHAPTER TWO: LITERATURE REVIEW

## 2.1. Introduction

As digital technology has advanced over the past 50-odd years with a force unprecedented in history, governments, businesses and people around the world have been affected immeasurably (Fraser, 1996). Fraser argues that, the already enormous and exponentially growing capacities for electronic storage, transmission and rapid manipulation of binary data changed the modern landscape virtually overnight, making the world of today's children unrecognizable in many ways to those of earlier generations. By the year 2005, the Commerce Net Research Council (2000) estimates there will be over 765 million Internet users. This wide use of computers and technology will create further challenges for the Government, industry and law enforcement personnel. Crimes associated with the theft of information, global terrorism and violence can now be conducted online.

A relatively new scientific discipline, known as computer forensics, was created in the mid-1990's to obtain computer evidence, which allows for this evidence to be admissible in court when prosecuting the cyber criminal. However, such fundamental restructuring in society also results in certain disadvantages, on all levels. Our vulnerability increases with the perceived value of and reliance on this technology. Increased opportunities for the industrious to be more productive also allow the less-upright new avenues for malevolence. Coupled with the fascinations of our Information Age, the world of criminal justice provides an interesting vantage point to assess how our complex community tries to restrain itself while racing into the future (Gilmore, 2001). It, therefore, remains to be seen whether the current approaches to deter and redress cyber crime will yield any results.

### 2.1.1. Computer Forensics

Various scholars have defined computer forensics. The Department of Justice (DoJ) Federal Bureau of Investigation (FBI) (Forensic Science Communications, 2000) defines computer forensics as: "The Science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media". Additionally, the DoJ/FBI includes in the definition of computer forensics as "the principles of the science of computer forensics includes the formalized and approved methodology to collect, analyze and present data in a court of law." Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically encoded information.

McKemmish, (1999) defines computer forensics as: "The application of computer investigation and analysis techniques in the interests of determining potential legal evidence. The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable." According to Farmer & Vennema (1999), computer forensics refers to: "Gathering and analyzing data in a manner as freedom distortion or bias as possible to reconstruct data or what has happened in the past on a system."

Chappell, (2000) defines 'Computer Forensics' as "the detailed examination of computers and their peripheral devices, using computer investigation and analysis techniques in the interests of determining potential legal evidence". The evidence to be found will cover a wide range of subjects and will not be limited to criminal offences. The information required may relate to such things as theft of trade secrets, theft or destruction of intellectual property, fraud, and other civil cases involving wrongful dismissals, breaches of contracts and discrimination issues.

### The Incident Response Plan

The relevant definition to be adopted in this study is that by Judd Robbins (Oseles, 2001), a prominent computer forensics investigator who defines it as "the application of computer investigation and analysis techniques in the interests of determining potential legal evidence." Other experts have taken the definition a step further, believing computer forensics has evolved into a science. Noblett et al. 2000, as well as the FBI, define computer forensic science as "the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media."

Basically, computer forensics is digital detective work. It is searching a digital crime scene for evidence, containing and preserving the evidence, analyzing the evidence, and then finally presenting the findings in legal proceedings and court. In other words, it is similar to performing an autopsy, except on a digital device versus a human body. It is important for organizations that face various computer threats in their operations to have the capacity to carry out computer forensics work.

Computer Forensics is involved in the investigation of the following types of computer-related crimes according to the FBI National Computer Crime Squad's (NCCS) list of crime categories it investigates listed as:

- i). Intrusions of the Public Switched Network (the telephone company);
- ii). Major computer network intrusions;
- iii). Network integrity violations;
- iv). Privacy violations;
- v). Industrial espionage;

- vi). Pirated computer software; and
- vii). Other crimes where the computer is a major factor in committing the criminal offense.

This chapter reviews the various practices involved in computer forensics. It will begin with a review of Incident Response and Legal Implications, a discussion of those areas, such as the incident response plan and related guidance, which must be actively utilized by an organization prior to attack. It will further present a review of the seven-step process and methodology for performing computer forensics on Information Systems, which allows for acquiring, preserving, retrieving, and presenting data in a court of law. Finally, there will be a review of the various Unique Challenges of Computer-Based Discovery that an organization may face in computer forensics exercises.

## 2.2. The Incident Response Plan

The topic of computer forensics cannot be broached without a discussion of an incident response plan, proper security policies and potential legal implications for a corporation. Whether a company is connected to the "Internet" or not, is not the question -- attacks to Information Systems can occur from within and from without (Gilmore et al., 2001). The Incident Response Plan is discussed within the context of the Information Systems Security plan of the organization, since computer forensics will fall within the domain of Information Systems security of the organization.

A Chief Executive Officer (CEO) can properly respond to an incident when (not if) it occurs, if the company is prepared. The old adage is appropriate in this case, according to Armstrong (2001), "proper planning prevents poor (incident response) performance." There is much at stake in company Information Systems and as much money, time and attention needs to be spent on policy creation, implementation and maintenance as to what a company devotes to network creation, implementation and maintenance. Just as computer hardware and software need protection, so do the assets and information that reside in the equipment which are of as much, if not greater value. "Probably, the best way to do this is by implementing incident response plans so that a security threat can be identified and dealt with quickly and effectively with no or minimum disruption to business," according to British Telecommunications Ignite Solutions (2001).

The new trend for incident response plans is to develop incident response teams. This approach is effective because handling an incident as a combined corporate effort eliminates

replicating work. According to Wack (1991), typical goals for the incident response team's plans include the following: -

- 1) A procedure for reporting incidents;
- 2) Sorting incidents by type of incident or technology affected;
- 3) Availability of technical assistance, if necessary;
- 4) Provide training and security awareness for users and vendors. "People are the single most important element of any information security program. Additionally, advise and frequently update people concerning threats, counter measures and their responsibilities," as recommended by E Biz Chronicle.com (2001);
- 5) Provide an information repository of relative security information;
- 6) Promoting related security procedures and policies, and, according to E-Biz Chronicle.com (2001), "Update, maintain, and routinely revalidate electronic security tools. This includes intelligence and early warning, authentication, encryption, intrusion detection and other tools;"
- 7) Develop and have ready to contact the appropriate law enforcement agencies and forensic response team; and
- 8) Finally, an Incident Response Plan Handbook is required to complete an incident response plan.

One of the most important aspects of the incident response plan is the contacts that a company develops with its local law enforcement and related investigative agencies knowing who to call when is key when handling any incident. Contacting the appropriate authorities initially can, according to Shipley (2001), "expedite...response to a crime scene. The easier..." a CEO "makes it for law enforcement, the faster a perpetrator will get arrested." According to Gilmore (2001), "An ill-prepared Executive with no formal corporate policy or plan for facing computer hacks and security breaches places the company in jeopardy and risks the corporate assets that they have been hired to protect." It is best to have an appointed liaison designated to work with law enforcement in case of a computer crime incident.

### **2.3. Computer Forensic Science: The Investigation Process**

Computer Forensics is increasingly being regarded as a science. As Villano (2001) says, "once regarded by technophiles as an obscure component of network security, the discipline has blossomed into a science of its own". Forensics specialists can draw on an array of methods for discovering data that resides in a computer system or recovering deleted, encrypted, or damaged file information.

One of the crucial aspects as well as a major challenge in computer forensics is not only finding, but also preserving electronic data, as electronic evidence is fragile, and can easily be modified and deleted. The most common legal difficulty faced by organizations seeking to redress cyber-crime in the court is having digitally based evidence accepted. Gathering legal evidence goes beyond normal data recovery. It is difficult to accomplish and requires trained specialists who know computers, the rules of evidence gathering, and how to work with law enforcement authorities (Walker, 2001).

One of the keys to effectively find and use electronic information is having an understanding of the kind of information that may exist, and where within the system to look for each type of information. Unlike paper evidence, computer evidence can often exist in many forms and locations within any computer system. Some of the main sources of electronic evidence are hidden, encrypted, and deleted data, e-mail, Internet files such as persistent cookies and cached files, and auditable events contained in system log files.

### **2.3.1. Electronic Types of Data**

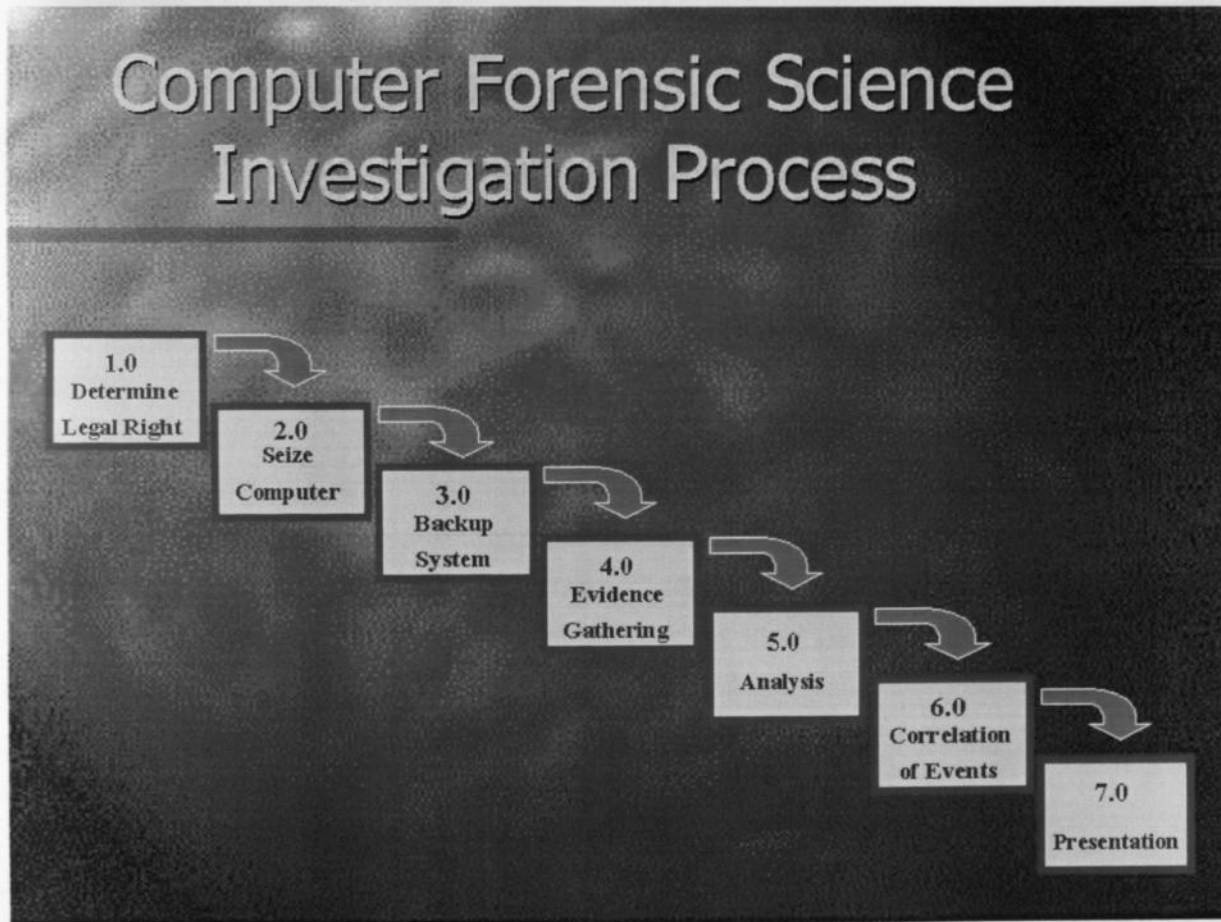
Active data is the information readily available and accessible to users like word processing documents or spreadsheets. Archival data is the information no longer in use, but stored separately to free space on a drive, while backup data is information copied to portable media. But it is within the so-called residual data where computer forensics focuses the most. Residual data is information that appears to be gone, but is still recoverable from the computer system. It includes "deleted" files found in the free space and data existing in other system hardware such as buffer memories. Residual data may also be found in the "slack space" on a disk. It is important to notice that a simple copy of the disk or drive will not capture this type of data. Making an image copy of the disk is the only way to capture residual data (Feldman et al., 2001).

Although data and electronic mail are usually the main sources of evidence that investigators look for, background information might also serve as a good source for electronic evidence. Background information can include the electronic audit trail created by auditable events in most network operating system (NOS) software. These audit trails and computer logs normally contain information about who accessed the system as well as when, where and how long a user was on the system. They also provide information about who modified a file last and when the modification was made. Audit trails may also indicate when and by whom files were downloaded to a particular location, copied, printed out or purged (Feldman et al., 2001).

## 2.3.2. Computer Forensics Process Methodology

To ensure that evidence is processed safely and to eliminate discrepancies in the industry, investigators follow a set of steps to safely retrieve electronic evidence for analysis. After researching the science of computer forensics, seven distinct steps need to be followed according to McPeak (2001), which the examiner must follow. These steps can be characterized into four functional areas: acquiring, preserving, retrieving or presenting evidence. The 7-step Computer Forensic Methodology process can be found in the diagram below:

*Diagram 1: Computer Forensic science Investigation process*



Source: *Computer Forensic Science: A methodology (McPeak et. al., 2001)*

### i.) Step 1 - Determine Legal Right

Prior to the onset of an investigation, it is extremely important to follow two steps, which are discussed further. First, the examiner must obtain authorization from the proper authorities, corporate and public sector legal departments. The examiner should always gather and preserve evidence according to basic rules of Evidence. This is an important step because without the appropriate authorization to evaluate computer resources, the evidence gathered might be rendered inadmissible in court. The next step is to contact appropriate law enforcement personnel. At this time, the company should engage its own approved forensic



team. The corporate legal, local law enforcement and forensic group should work as a team to ensure that the Rules of Evidence are adhered to when processing electronic evidence.

## ii.) Step 2 - Seize Computer System and Evidence

### a.) Document Hardware Configuration

Photographing the original hardware setup is the first step in proving that evidence was not altered, damaged or tainted. Before moving or dismantling the computer, it should be photographed from all angles to document the system hardware components and how they are connected (Betts, 2000).

### b.) Isolate System in Secure Area

The computer system should be immediately isolated and protected so only the forensic team examining the incident has access.

### c.) Chain of Custody

Wright (2001) defines the chain of custody and its importance in the computer forensic process as the following:

"A means of accounting for who has touched a given piece of evidence, when they touched it and what they did to the evidence. It's a way of demonstrating that evidence hasn't been damaged or tampered with while in the care of the investigator. In his book, **Criminalistics: An Introduction to Forensic Science**, Saferstein notes, "Failure to substantiate the evidence's chain of custody may lead to serious questions regarding the authenticity and integrity of the evidence and the examinations rendered upon it" As one would imagine, changes to the chain of custody can quickly ruin a case.

### d.) Document the System Date and Time

A software forensic tool can help in ensuring the accuracy of the dates and times associated with computer files, which could be critical from the evidence standpoint. This assists in avoiding courtroom discrepancies between system time and real time.

## iii.) Step 3 - Backup System

### a.) Boot Computer from a DOS Boot Diskette

The following step could present a true challenge, as there is a significant risk involved of losing data. Often, the hardware configuration is unknown; therefore, it is imperative to boot the system using an external boot device such as a floppy, CD-ROM or USB peripheral. This guarantees that the internal drive remains intact and no processes access it. According to Pettis (2001), the vice president of Information Systems Security Association, there are two

methods for protecting the evidence - either booting the machine from an external device or removing the hard drive completely. These two methods are detailed further.

#### **b.) Mirror Image/Bit-Stream Backup of Suspect Drive**

The step involves using a software package that allows creating a complete bit-stream backup mirror image of the target drive. Such mirror image backups exactly replicate all sectors on an internal storage device. This image is mounted as read-only, allowing an examiner to drill down and evaluate contents in a Windows Graphical User Interface (GUI) without disturbing actual files – including critical data and time stamps. The image is continually verified through cyclical redundancy checksums and Message Digest 5 (MD5) hashes since the accuracy is critical to the success of the operation. This provides mathematical authentication on all storage devices Information Security, (2001).

#### **c.) File Slack Backup**

New Technologies (2001) defines slack space as the remnant area at the end of the file. It is also important to use the software to collect all of the disk space from the end of the files to the end of the cluster. This space might have been used to hide information. Disk space can be searched for words or phrases that could be associated with the case. Data can be found in special (and typically inaccessible) areas of a disk. This includes but is not limited to what is called 'unallocated' space on a disk (currently unused, but possibly the repository of previous data that is relevant evidence), as well as slack space in a file (the remnant area at the end of a file, in the last cluster). The findings can be viewed with several viewing tools, including Symantec Norton Disk Utilities.

### **iv.) Step 4 - Gather Evidence**

#### **a.) Searching Techniques**

With a mixture of background investigation, deductive reasoning and common sense, investigators can come up with a list of key words to start the search. At this stage, forensic software tools can be of great help, as it would be impossible to manually search for every file in the system. Unallocated space and slack space – defined above- are some of the places where investigators concentrate when looking for relevant information.

**Define Key Words:** - With a mixture of background investigation, deductive reasoning and common sense, the investigator can come up with a list of key words to start the search (Betts, 2000). Forensic software tools can help in searching files that otherwise would be impossible to manually search given the capacity of modern hard drives.

**Define Free Space:** - When a file is "deleted" the data in that file is not erased. Rather, the computer marks the file space as "free". Data in a deleted file is not erased until it is overwritten with data from a newly saved file or until it is "wiped" by specialized programs. Until data is overwritten or wiped, it can be restored through use of undelete or salvage commands, available in the operating system or using special software. Once the free space is located, text search features of the software tool can be used to find specific information (Feldman and Rodger, 2001).

**Search for Hidden Information:** - Another place to look for hidden information is the slack space on a disk. Slack space is created because DOS will only store the data from one file per cluster (one of a system of data compartments on a disk). The unused portion of a cluster is referred to as slack space. If a new file overwriting a delete file contains less data than the deleted file, there may be a file fragment left in that slack space. This space may have been used to hide information. The slack space is then searched for words associated with the particular case (Feldman and Rodger, 2001).

**Search for Deleted Files:** - New Technologies (2001) provides a detailed explanation of deleted file searching, which is presented below.

"When files are erased or deleted in DOS, Windows, Windows 95, Windows 98 and Windows NT, the content of the file is not actually erased. Unless security grade file deletion software is used, data from the 'erased file' remains behind in an area called unallocated storage space. The same is true concerning file slack that may have been attached to the file before it was deleted. As a result, the data remains behind for discovery through the use of data recovery and/or computer forensics software utilities.

Unallocated file space and file slack are both important sources of leads for the computer forensics investigator. The data storage area in a factory fresh hard disk drive typically contains patterns of sectors, which are filled with patterns of format characters. In DOS and Windows-based computer systems, the format pattern for a floppy diskette usually consists of binary data in the form of hex F6s. The same format pattern is sometimes used in the format of hard disk drives but the format patterns can consist of essentially any repeat character as determined by the factory test machine that made the last writes to the hard disk drive. The format pattern is overwritten as files and subdirectories are written in the data area.

Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files, which were transparently created and deleted by computer applications and

also the operating system. All of such files and data fragments can be sources of computer evidence and also security leakage of sensitive data and information."

### **b.) Audit Trails and Automated Methods for Discovery**

Microsoft recommends (Microsoft.com, 2001) some best practices for discovering information in audit trails and other files. Many operating systems enable monitoring of accesses to specific objects, such as files and directories, registry keys, directory service objects, and kernel objects. Auditing is frequently set on a per-object and per-access basis. In other words, the administrator specifies which objects to audit and which accesses of those objects to audit. Auditable accesses vary among different object types and correspond with the permissions that can be assigned to that class of object.

When auditing, it is important to utilize a targeted approach. The administrator should determine the minimum number and type of objects that are to be audited and then determine the minimum number of accesses that must be monitored for each type of audited object. An overly broad approach to auditing will have a significant impact on the system's performance and will result in the collection of more data than is necessary or useful. Conversely, an audit approach that does not capture enough events will not allow for a successful analysis of events.

### **c.) E-mail Forensic Techniques**

According to New Technologies, Inc. (2001), a new type of virtual evidence has been created as a result of e-Commerce transactions and e-mail communications over the Internet. Computer-related investigations can involve the review of e-mail folder archives to determine Internet policy abuses in businesses or government agencies. Using computer forensics procedures, processes and tools, the computer forensics specialist can identify fragments of e-mail messages that were dumped from computer memory during past work sessions. When such leads are identified, they can be perfected through the use of forensics text search programs.

### **d.) Internet Forensic Techniques**

Because MS DOS and MS Windows were never designed to be secure, computer forensic scientists and law enforcement personnel will find it easy to obtain information about Internet content, web browsing and other activities from MS Windows systems. Even after data has been deleted, much information remains available for discovery in the form of cache, cookies and other browser files, and Windows swap files. Often the obvious files, such as a Netscape web browser's cache files, cookies and bookmarks have been deleted by the offender, leading the computer forensic scientist to explore other less obvious computer resources to obtain

evidence of illegal activity. One primary resource for computer evidence is the discovery of the Windows swap files.

Windows swap files are dynamically created during the web session and then erased. These same files are then left behind as a large erased file in unallocated space. Unless specifically defragmented and written over, these erased swap files can be retrieved and archived for analysis.

### e.) Password Cracking Techniques and Cryptanalysis

Cryptanalysis can be an invaluable tool to the computer forensics scientist in order to penetrate encrypted files and passwords. Cryptanalysis is one of two branches of cryptology that is concerned with breaking and defeating cryptography (R. Summers, 1997). A cryptanalyst is the attacker, or in this case, the computer forensic scientist that is concerned with eavesdropping and breaking encrypted cipher text.

Often, computer forensic personnel have found files encrypted on systems under investigation hence hampering investigation. Another problem facing computer forensic scientist is cracking files protected by passwords.

### v.) Step 5 – Analysis

Because of many variables such as computer systems, applications, media and type of incident under investigation, there is no single best practice on what should be analyzed. However, Sommer (1997) provides a number of methods that a computer forensic scientist should consider when evaluating a system under investigation. Some of Sommer's analytical methods are presented in Table 2.

**Table 2: Computer Forensic Analytical Methods**

<b>Review and Examine:</b>	<b>Report:</b>
All media	All media
Back-up and archived files	Sources of back-up and archived files
Suspect computers and systems for "proper" working during relevant period, including service logs, fault records, etc.	On the setting up of pro-active monitoring in order to detect unauthorized or suspect activity within or across: <ul style="list-style-type: none"> <li>- Applications programs</li> <li>- Operating systems</li> <li>- Local area networks</li> </ul>

Step 6 - Correlation of Events	- Wide area network - e-mail and other app. protocols
Establish Timeline	
Reviewing of access control services - quality and resilience of facilities (h/w and s/w, identification /authentication services)	Use of special "alarm" or "trace" programs
Review of system / program documentation for: design methods, testing, audit, revisions, and operations management.	Use of routine search programs to examine the contents of a file
Reviewing of applications programs for "proper" working during relevant period, including service logs, fault records, etc.	Use of purpose-written search programs to examine the contents of a file
Identification and examination of audit trails	Event reconstruction
Identification and review of monitoring logs	Complex computer intrusion
Telecommunication call path tracing (utilities companies only)	Complex fraud
Reviewing and assessment of access control services - quality of security management	System failure
Reviewing and assessment of encryption methods - resilience and implementation	Reverse compilation of suspect code
Reviewing and assessment of measuring devices, etc. and other sources of real evidence, including service logs, fault records, etc.	Disaster affecting computer driven machinery or processes
Examination of telecommunication devices, location of associated activity logs and other records perhaps held by third parties	Inter-action with third parties, e.g. suppliers, emergency response teams, law enforcement agencies
Use of computer programs which purport to provide simulations or animations of events: review of accuracy, reliability and quality	Safe seizure of computer systems and files, to avoid contamination and/or interference
Estimating if files have been used to generate forged output	Safe collection of data and software
Proving / testing of reports produced by complex client / server applications	Safe and non-contaminating copying of disks and other data media

**Source: Sommer, Peter (1997)**

## **vi.) Step 6 - Correlation of Events**

### **a.) Establish Timeline**

It is necessary to establish the time line since the computer file dates and times can be extremely important as evidence. It should be verified whether the system time was configured for the proper time zone and/or daylight-savings time. For example, if the system/BIOS clock is off one hour, all the files will have time stamp with one-hour delay.

### **b.) Correlate Events and Reconstruction**

Because of the complexity of computer systems and the mystery of the incident, event reconstruction and correlation can be one of the most difficult tasks facing a computer forensic scientist. Sommer, (1997), provides an excellent description of how to present event reconstruction and correlation.

...Show a sequence of events or transactions passing through a complex computer system. This is related to the proving of electronic transactions but with more pro-active means of investigation event reconstruction - to show how a computer installation or process dependent on a computer may have failed. Typical examples include computer contract disputes (e.g. when a computer failed to deliver acceptable levels of service and blame must be apportioned), disaster investigations and "failed trade" situations in securities dealing systems

Often, events are related to time, and can be measured anywhere from minutes to months. When time has been established, the computer forensic investigators should correlate incidents with forensic findings to prove or disprove a theory.

## **vii.) Step 7 – Present Evidence**

Computer Law Associates (CLA, 1996) discusses the importance of computer forensic evidence and record credibility in the courtroom. The main question that judges wish to know is whether the records are reliable. The computer forensic scientist, being used as an expert witness or otherwise, must convince the judge that the computer evidence was not mishandled or not kept secure. Although there are different types of computer and applications, which make for the creation of a single framework for presenting computer evidence in court difficult, the following rules apply. First, document the entire computer forensic process from the initial notification of the incident through isolation of the system. Particular attention should be made on how the system was isolated and protected, to how only copies of disks were searched and viewed. The original disk and data should never be tampered with. Second, document what was examined. This should include discussions of all disks, directories and files. Also, hidden, deleted and encrypted files should be discussed. Next, document what was found and where.

Fourth, document what was done to recover the data. This step should include the text search process previously described. Finally, printout and inventory all applicable records that will be admissible in court.

## **2.4. Unique Challenges of Computer-Based Discovery**

Though computer-based discovery has many potential advantages, it can raise unique issues that normally do not occur or are less problematic in conventional, paper-based discovery. Among the most common difficulties are: The preservation of data subject to discovery; the location and volume of data; e-mail as a novel medium; documents that have been deleted from the computers; backup tapes, archives, and legacy data; the conduct of on-site inspection; the form of production; and the need for expert assistance.

### **2.4.1. Preservation of data**

In conventional paper-based discovery, the documentary sources of information have been, for all intents and purposes, physically stable. Attorneys seldom have cause to assume that paper or microfilm files are subject to imminent damage or destruction. Fire, flood, or corporate document destruction procedures occasionally result in the loss of potential evidence, but these have relatively rare occurrences.

On the other hand, information stored in electronic form is easily changed, overwritten, or obliterated by everyday use of the computer, whether it is a single desktop PC (personal computer) or an enterprise-wide network. The simple acts of booting up a computer, opening a file, adding new data onto a hard disk, or running a routine maintenance program on a network can alter or destroy existing data, without the user's knowledge. At the outset of litigation involving computer-based discovery, attorneys on both sides have a heightened responsibility to inform their clients of the duty to preserve potential evidence. Again early in the case, the parties should meet and try to agree on the steps each will take to segregate and preserve relevant data, to avoid later accusations of spoliation.

### **2.4.2. Location and volume of data**

Overly (1999) argues that in the days of conventional paper-based discovery, most organizations had centrally located files or a limited number of physical file locations. According to Overly, in the PC-based world, each employee may have a desktop computer, plus disks or other removable data storage media, a laptop computer, a home computer, and a hand-held personal organizer, all containing potentially relevant data. Larger organizations will have network servers connecting and storing data for many PCs, plus backup and archival data



storage. Offsite and even offshore data storage facilities, Internet service providers, and other third parties may also hold data subject to discovery. Given all this, the cost and complication of conducting discovery in a modern, distributed business-computing environment can be enormous.

In paper-based record-keeping systems, outdated records, papers with no business significance, and superfluous copies are destroyed routinely. Records managers maintain paper files in "business-record order." According to a survey (1998), conducted by the American Bar Association and the American Corporate Counsel Association, in computerized business environments, equivalent electronic records management systems seldom exist. Copies of documents are made routinely, distributed widely, and seldom purged when outdated. Still on the same issue, Gahtan (1999) states that, potentially discoverable records are stored according to computer logic, as opposed to "business-record" logic, and can be difficult to locate and untangle from irrelevant and privileged records. The attorneys, therefore, have an obligation to investigate their clients' Information Management System thoroughly to locate potentially relevant and discoverable material, no matter how technically opaque that Information System appears.

### 2.4.3. E-mail as a unique phenomenon

Electronic mail does not have a counterpart in the conventional paper-based world. Several characteristics make e-mail particularly problematic. One is the sheer volume, which can be staggering, even for a small company or individual. Another is the lack of a coherent filing system, as e-mail systems are seldom designed for file management and retrieval. Supra (1998) notes that relevant business-related e-mail messages will be found side by side with irrelevant and often very private personal e-mail messages. Solomon (1990) in his article ***"Workplace: As Electronic Mail loosens Inhibitions, Impetuous Senders feel Anything Goes"*** argues that perhaps the most important characteristic of e-mail is the nature of the medium itself, which commentators in both the popular press and the legal literature have noted is informal, breezy, and riddled with slang, jargon, and jokes, even in the strictest business environments.

Seed (1999) notes that, the above factors of the e-mail combine to make retrieval of e-mail messages by topic difficult, even with computer-based word-searching, and screening for relevance and privilege costly and time-consuming. But these characteristics of e-mail also make it a most attractive target for discovery. Conventional document-intensive discovery may present problems of volume and density, but generally the organizational system of paper files, where one exists, can be understood without any special technical skill or knowledge

#### **2.4.4. Deleted documents**

According to Johnson (1998), in the conventional paper-based world, once a document is shredded or incinerated, it is no longer subject to discovery as a practical matter. However, the routine "deletion" of a computer-based document does not destroy the data. Hitting the "delete" key merely renames the file in the computer, marking it available for overwriting if that particular space on the computer's hard disk is needed in the future. The data may remain on the hard disk or on removable storage media for months or years, or may be overwritten only partially.

It is a relatively simple task for a computer forensics expert to restore routinely deleted data, but it is expensive and the results are uncertain. Therefore deleted documents represent a potential increase in the volume of discovery, with associated increases in cost and delay.

#### **2.4.5. Backup tapes**

Most businesses, as well as many individuals, periodically back up their data onto tapes or disks for disaster recovery purposes. Often these tapes are kept for months or even years. Data and documents that have been edited, deleted, or written over in the normal course of business may be recovered from these tapes or disks. Andy Johnson (1998) notes that Backup tapes, are however not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. Therefore, the organization of the data mirrors the computer's structure, not the human records management structure, if there is one. Special programs may be needed to retrieve specific information, and the process may be costly and time consuming (Bruce Rubinstein, 1997).

#### **2.4.6. Archives and legacy data**

Ideally, archival electronic files should be organized for identification and retrieval of individual documents or series of records. Ideally, as businesses, institutions, and government agencies adopt new computer systems, the data from older systems should be transferred to new media. In reality, such electronic records management processes are primitive or non-existent in many organizations. It is common to find that: unorganized backup tapes are kept as a substitute for organized archival files, old data are impossible to read using current hardware and software, old data transferred to current media and format have lost important elements necessary to establish context or authenticity. (Supra, 1998)

## 2.4.7. On-site inspection assistance

Computer-based discovery makes on-site inspections particularly problematic. On the one hand, it may be necessary to view the computer system in operation to make sure the discovery protocols are being performed properly, to check the adequacy of security and chain of custody, or to ascertain the provenance of computer records. On the other hand, the nature of computer record storage and organization makes it virtually impossible to protect privileged or trade secret information in the context of an on-site inspection, and any manipulation of the computer by the opposing party, counsel, or expert may compromise the entire process.

D. Colo (1996) states that, in *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, a botched on-site inspection resulted in the loss of possibly critical data by the party-seeking discovery. Discovery had been protracted and acrimonious in this trade secret theft case when the plaintiff learned that an individual defendant had allegedly destroyed records on his computer. The plaintiff obtained a "Site Inspection Order" designed to allow it complete access to the defendants' computers, while protecting the defendants' rights to object to the production of irrelevant or privileged materials. As a result, the plaintiff documented several instances of what it characterized as destruction of evidence, but the magistrate judge denied most of the plaintiff's motion for sanctions, citing the behavior of the plaintiff's own expert. For instance, to examine one particularly important computer, the expert used a program that erased, at random, 7 to 8 per cent of the information that might otherwise have been available. The expert also failed to obtain and preserve the creation dates of essential files and failed to use accepted computer evidence preservation procedures. The cost of an on-site inspection in terms of business disruption must be considered. It is one thing to inspect a conventional file room or document warehouse. The use of paper files for short periods of time does not generally affect ongoing business operations.

## 2.4.8. Form of production

Over a long time, the typical and preferred response to a computer-based discovery request has been a printout of the computer data. This is because for many years, few if any law offices had computers, and the software necessary to translate and manipulate the data was not mass marketed. Today, producing printouts of computer data is so unnecessary that it might be considered an abusive tactic. Many computer-based documents, such as relational databases and spreadsheets, are meaningless in printed form. The recipient is forced to reenter the data or spend long hours performing manual analysis. Electronic exchange of computer data is a preferred mode, although plenty of room exists for dispute over the exact format (Adams, 1972).

#### **2.4.9. Need for expert assistance**

As demonstrated in earlier discussions, both parties engaged in computer-based discovery will need the assistance of computer experts. This is costly, but in the long run may save costs and time. According to Joan Feldman and Andy Johnson, once the experts have had an opportunity to assess their respective parties' computer systems and capabilities, they will be in a much better position than the attorneys to negotiate the technical aspects of conducting discovery, including search protocols, privilege and relevance screening, and production. Often the lawyers can be taken out of the picture entirely. In many cases, the experts on opposing sides will have to meet and work out agreements on the exchange of computer system information, the procedures for inspection, the search terms each side will use, and other details best left to those with technical knowledge and experience.

### **2.5. Overview of the Banking sector**

The banking sector comprises 49 financial institutions with 41 commercial banks, 2 non-bank financial institutions (NBFIs), 2 mortgage finance companies and 4 building societies (Monthly economic review; June 2004 issue). According to the Central Bank of Kenya, during the year to May 2004, the balance sheet of the banking industry expanded with total assets increasing by 14.2% to Ksh. 542.2 billion by the end of May 2004 from Ksh. 474.7 billion in May 2003. The sector recorded an improved performance in 2003 with net profits increasing by 134% from Ksh 6bn in 2002 to Ksh 14.1bn. According to an Annual Bank Supervision report (2003), the Kenyan economy recovered to expand in real terms by 1.8 % in 2003 compared with 1.1.% in 2002 and 1.2% in 2001. The economic expansion was broad based but driven mainly by the agricultural and services sectors and partly reinforced by strong macro economic fundamentals.

The banking sector has embraced changes occurring in Information Technology with most banks having already achieved branchless banking. According to The Central Bank Annual Supervision report (2003), the increased utilization of modern information technology has for example led to several banks acquiring ATMs as part of their branchless development strategy measures. The Central Bank notes that, advancement in Information and Communications Technology (ICT) in the banking industry has enhanced efficiency and improved customer service. This is reflected particularly in the increased use of ATM cards resulting from broadening of ATM network, including additional ATM machines and a wider network of merchants that accept payment through credit/debit cards. According to the report, the total number of ATMs in the industry as at 31st December 2003 was 230 compared with 166 as at end of December 2001. The number has since increased with the implementation of Kentswitch,

a Shared ATM network comprising a consortium of eighteen small and medium sized banks, which went live in December 2002.

### Research Design

Several banks have also entered into the Internet Banking and established websites. Internet banking however is still at its infancy and more in terms of utilization is expected in this sector. Additionally in May 2004, VISA estimated that the use of Visa cards had increased by 43 per cent in Kenya last year, which translated to US\$452 million growth. They noted that in 2003, the number of Visa and Visa Electron cards issued by Visa member banks in Kenya rose to over 557,000. They described Kenya as the fastest growing market in Africa, outside South Africa. According to the Bank Supervision report (2003), this progress has, however, been accompanied with increased operational risks related to card frauds and Information Systems frauds. There is therefore the need for well-formulated ICT strategies and security policies to mitigate the possible attendant risks.

## 2.6. Conclusion

Computer forensics (collecting electronic evidence) is no trivial matter. Its purpose is to collect evidence from computer systems and computer media that can be preserved and analyzed by the investigator, and can be presented in court to aid in prosecution of criminals. In this process, there are many complexities that must be considered and the investigator must always be able to justify their actions.

However going by the trends in last decades where the use of computers and related devices is ever-increasing, Computer Forensic will become more and more important as Criminals will forever use computers to carry out a variety of crimes, from viral attacks, to financial fraud. It is imperative therefore that the legal and information professional fraternities know and understand the area as well as the challenges involved and ways of mitigating. Trained computer forensic professionals in both law enforcement and private industry will hence prove to be extremely valuable in the years to come for the fight against cyber crime to be won.

### Data Analysis

collected shall be edited for accuracy, uniformity, consistency and completeness and to enable coding and tabulation before final analysis (Cooper and Emory, 1998). It will be presented through the use of summarized percentages, proportions and tabulations in two sections of the questionnaire. Mean scores and standard deviations will be

# CHAPTER THREE: RESEARCH METHODOLOGY

## 3.1. Research Design

A census survey of the Banking Industry will be conducted. The study will therefore adopt a cross-sectional design with the respondents being the senior- most Officers in charge of the Information System Audit function in the various banks.

## 3.2. The population

The study focuses on all the 42 commercial banks (Monthly economic review; June 2004 issue -Appendix 3) in Kenya because it is presumed that each of the commercial Banks have heavily employed technology in their day to day operations and have at one time had a computer related crime committed hence has up to some extent adopted computer forensics practices in litigation support. The unit of analysis is the Bank itself as will be presented through the relevant management staff. The study aims at doing a Census of the entire banking sector. Census is the only complete snapshot in time hence the reason it has been selected for this study.

## 3.3. Data Description and Collection

Primary data will be collected for the purpose of this study. It will be collected using the self-administered questionnaire. The questionnaire will be semi-structured, having both open-ended and closed-ended questions. It will be administered to the Manager- Information systems Audit of each bank at their offices. The administration of the questionnaire will be by the "drop & pick later" method.

The questionnaire is divided into two parts. The objective of the first part is getting the demographic information on the Bank that is deemed relevant for the study. The second part of the questionnaire will be used to examine the existence of computer forensics practices; extent of awareness/adoption of computer forensics as well as the various challenges faced by the various banks in utilization of Information Systems evidence after a system compromise. The 5-scale Likert type scale will be adopted for the study.

## 3.4. Data Analysis

The data collected shall be edited for accuracy, uniformity, consistency and completeness and arranged to enable coding and tabulation before final analysis (Cooper and Emory, 1998). It will mainly be presented through the use of summarized percentages, proportions and tabulations in all the two sections of the questionnaire. Mean scores and standard deviations will be

evaluated and ranked to give the relative importance of the various computer forensics practices. Specifically, part of section II will be analyzed through the use of factor analysis.

Factor analysis is a systematic, statistical procedure used to uncover relationships amongst several variables. This procedure enables numerous correlated variables to be condensed into fewer dimensions known as factors. In the context of this research, the variables are the degree of agreement with various specific perception statements while the factors are the general underlying constructs. The factor analysis for this research will be conducted using a statistical package SPSS. The purpose of factor analysis is to discover simple patterns in the pattern of relationships among variables. In its procedure, rotation is applied to identify meaningful factor names or descriptions. A rotation, which requires that the factors remain uncorrelated, is an orthogonal rotation, while a rotation, which requires the factors to be correlated, is called Oblique rotation.

In this study, oblique rotation using Promax was carried out because the proposed framework indicates that the underlying constructs and variables are inter-correlated. Factor rotation is used to re-orient the factor loadings so that the factors are more interpretable. Use of Oblique rotation allows for correlations between factors since many attitudinal dimensions are in fact likely to be correlated. For easier interpretation of the factors, only the pattern matrix is examined (Rummel, 1970). The factor extraction method adopted for this study is principal axis factoring. Principal Axis Factoring, unlike principal component analysis, relaxes the assumption that the communality is equal to one. As a result, using this method enables the factor loadings to be higher, which leads to greater interpretability.



# CHAPTER FOUR: DATA ANALYSIS & FINDINGS

## 4.1. Introduction

This section provides the data analysis and findings of the survey. The data is analyzed using frequencies, means, standard deviations and factor analysis. It is presented in tables, pie charts and graphs. Part I was analyzed using proportions i.e. percentages, means and standard deviations. Part II was analyzed using factor analysis so as to reduce the variables to the underlying factors. Variables in Part II were assumed to be correlated and therefore the factor analysis procedure used was the principal axis factoring with promax rotation.

## 4.2. Bank demographic information

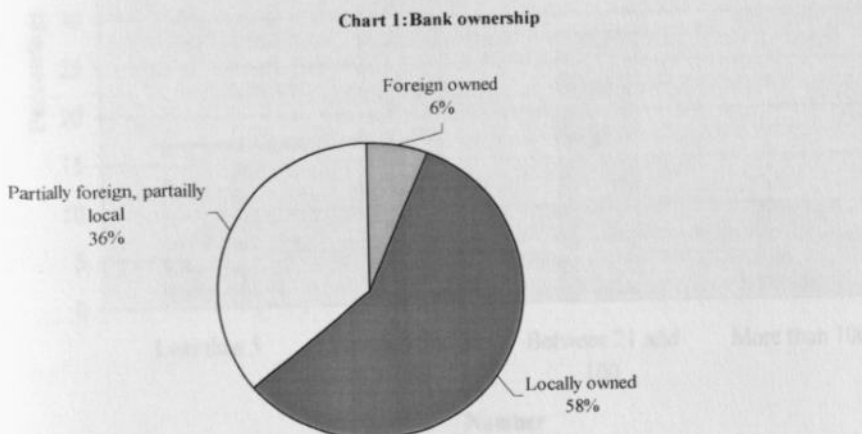
The variables considered in this section were mainly aimed at providing insight information of the various stakeholders in the banking industry. The aim of the information being to establish if any relation exists between the various stakeholders and employment of computer forensics as a discipline in the various banks.

### 4.2.1. Response rate

A total of 42 questionnaires were sent out and 29 were returned. The survey therefore achieved a return rate of 69%. This was considered adequate for the purposes of the study.

### 4.2.2. Ownership of banks

Majority of the banks in the survey (58%) are locally owned whereas 36% have partially foreign and local ownership and 6% are foreign owned as shown in chart 1 below: -





### 4.2.3. Customer base

Majority of the banks surveyed (66%) have a customer base of over 100,000-whereas 17% less than 20,000 and 100,000 respectively as shown in table 3 below.

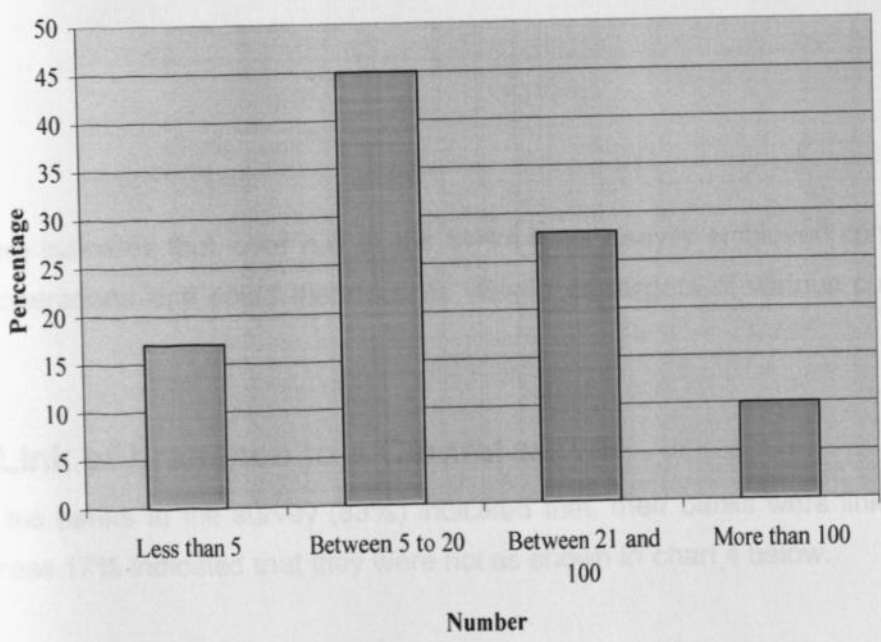
**Table 3: Customer base**

(In 000')	Frequency	Percentage
Less than 20	5	17
Less than 100	19	66
More than 100	5	17
<b>Total</b>	<b>29</b>	<b>100</b>

### 4.2.4. Number of branches

In terms of branch network, 17% of the banks have less than 5 branches, 28% have between 5 to 20 branches; 45% have between 21 and 100 branches; while 10% have more than 100 branches as shown in chart 2 below.

**Chart 2: Number of branches**



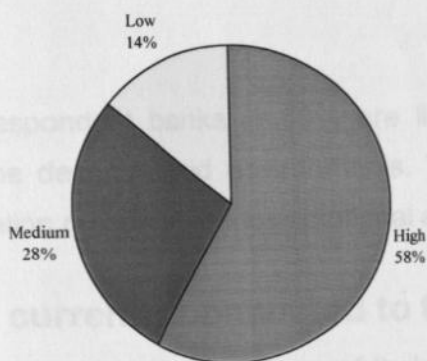
### 4.3. Use of Information Technology in the Banks

To establish the level of awareness of computer forensics within the banking sector, the respondent banks were requested to fill in various variables related to the deployment and use of computers in their banks. The response was as presented below: -

#### 4.3.1. Level of information technology use

In a majority of the banks (58%), Information Technology is highly used in the Bank's Operations and in 28% of the banks use of IT is medium and in 14% of banks use of IT is low as indicated in chart3 below.

Chart3:Level of Use of IT in the Banks

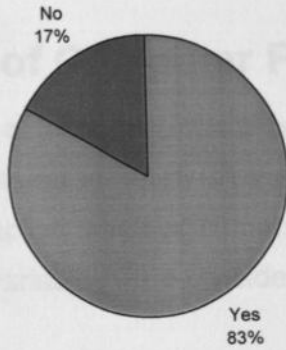


This therefore indicates that, over half of the banks have heavily employed computers in their day-to-day operations and could therefore be viewed as targets of various computer related crimes.

#### 4.3.2. Link of branches to a Central server

Majority of the banks in the survey (83%) indicated that, their banks were linked to a central server whereas 17% indicated that they were not as shown in chart 4 below.

Chart4:Link of branches to a central server

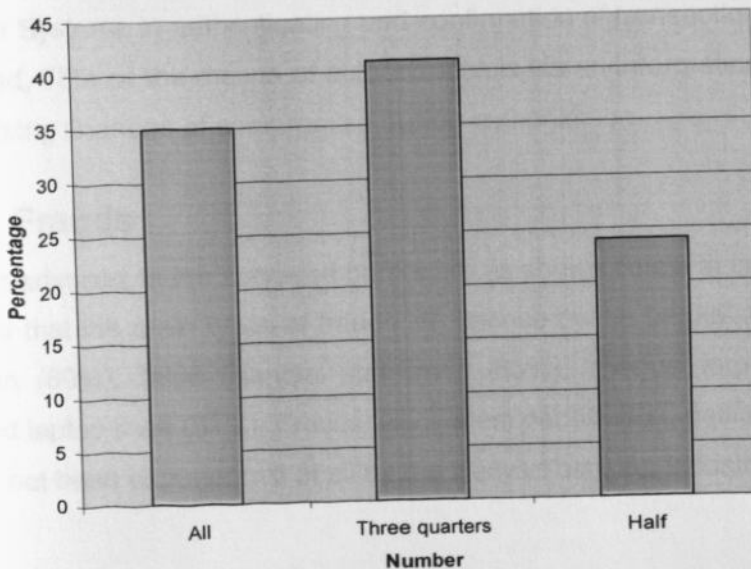


Majority of the respondent banks i.e.83% are linked to central server; clearly depicting a departure from the decentralized environments. This indication here is that, there is heavy sharing of information resources hence additional exposure to computer crimes.

### 4.3.3. Staff currently connected to the central server

In 41% of banks surveyed, three quarters of their staff are connected to the central server, in 35% of the banks all their staff are connected to the central server; and in 24% of the banks only half of the staff are connected as shown in chart5 below.

Chart5:Number of staff connected to a central server



There is a heavy indication of information sharing within the banking industry hence presenting more chances/risks of information resources being accessed by unauthorized users and probably put to alternative uses other than their original use.

## 4.4. Existence of Computer Forensics

Computer forensics is a fairly new discipline that has over the years grown tremendous as computers are encountered in nearly all sectors as tools of trade. The questions under this section sought to establish whether computer forensics really exist in the Kenyan banking industry. A number of variables were considered and are presented below: -

### 4.4.1. Transaction authorization methods

Majority of the respondents (57%) indicated that, they used both online and real time methods, 21% indicated that they use manual authorization; 14% use batch authorization and 7% use online and not real time authorization as indicated in the table below.

*Table 4: Transaction authorization methods*

Authorization method	Percentage
Manual authorization	21
Batch authorization	14
Online not real-time	7
Online and real-time	57
<b>Total</b>	<b>100</b>

The various transaction authorization methods indicate a fairly good level of dependency on Information Systems in authenticating and confirmation of transactions. While the methods may seem varied, 78% of the means of authorization is via an information system while 21% only is manual raising chances of compromise during authorization.

### 4.4.2. Frauds

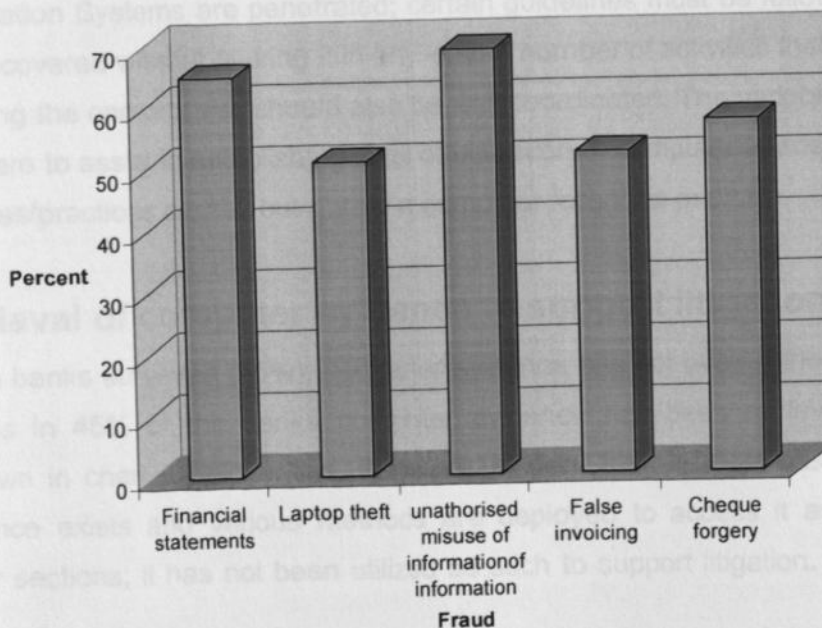
Frauds experienced in the surveyed banks are as shown below in table 5. From this table it can be inferred that the main types of frauds experienced by the banks are: Unauthorized misuse of information (69%), false financial statement (65%), cheque forgery (57%), false invoicing (52%), and laptop theft (51%). Frauds like system penetration, denial of service, and active wire trap have not been experienced at all by the Kenyan banking industry.

**Table5: Types of frauds**

Fraud	Percentage
1. Corporate espionage	21
2. Active wiretap	0
3. Credit card fraud	45
4. False financial statements	65
5. Hacking for financial/transactional fraud	14
6. Cheque forgery	57
7. Unauthorized misuse of information	69
8. Electronic and telecomm fraud	21
9. False invoicing	52
10. Secret commission/bribery	24
11. System penetration (e.g. web defacement)	0
12. Laptop theft	51
13. Inside abuse of information system	45
14. Denial of service	0
15. Misuse of General Ledger accounts	31

The top five frauds are unauthorized misuse of information accounting for 69%, false financial statements (65%), cheque forgery (57%) false invoicing (52%) and laptop theft (51), as can be seen in chart 6 below.

**Chart6:Top five frauds**



### 4.4.3. How frauds were discovered

The various frauds experienced by the banks in the survey were discovered in various ways as listed below in table 6. The most notable ways in which the frauds have been discovered include going through internal records (69%) and employee investigation (55%). The other methods include third party investigations (48%), internal auditor reviews (41%) while notification by customer accounts for 31%.

*Table 6: How frauds were discovered*

Method of discovery	Percent
Third party Investigations	48
External auditor review	21
Employees investigation	55
Notification by suppliers	0
Notification by authority	0
Notification by customer	31
Internal records	69
Internal auditor review	41
Anonymous letter/informant	7
Management investigation	0

Given that going through internal records accounts the highest percentage, it is possible therefore to have frauds perpetuated and records destroyed to conceal evidence.

### 4.5. Computer forensics practices

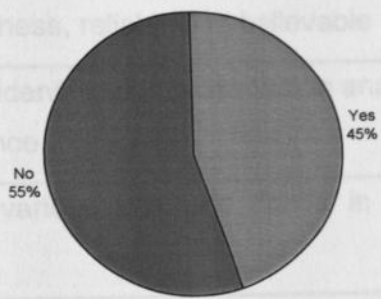
Whenever Information Systems are penetrated; certain guidelines must be followed to ensure the evidence is recovered without altering it in any way. A number of activities that are expected to happen following the compromise should also be well coordinated. The variables considered for this section were to assist in establishing level of utilization of computer forensics in litigation and the procedures/practices carried out during a computer forensics exercise.

#### 4.5.1. Retrieval of computer evidence to support litigation

In majority of the banks surveyed (55%), computer evidence has not been retrieved to support litigation whereas in 45% of the banks computer evidence has been retrieved to support litigation as shown in chart 6 below. It is, therefore, evident that, in most cases though the computer evidence exists and various methods are deployed to access it as indicated by results of earlier sections; it has not been utilized as such to support litigation. It is, however,

important to note that, the utilization of such evidence is growing as is indicated the percentage of banks that are indeed going in to the retrieval of such evidence.

Chart6: Retrieval of computer evidence



**4.5.2. Type of computer evidence retrieved to support litigation**

In majority of the banks surveyed (76%) real evidence (logs) were retrieved and used to support litigation. 24% of the respondents did not indicate the type of computer evidence they used to support litigation as shown in table6 below. This means that, real evidence (production of computer logs) is the most popular method used to support litigation. Methods such as Testimonial (evidence supplied by a forensic expert) and Hearsay (evidence supplied by a person who was not a direct witness) are still to be explored in the Kenyan Banking industry.

Table7: Type of computer evidence

Evidence	Percentage
Not indicated	24
Real evidence (logs produced)	76

**4.5.3. Extent to which the various evidence gathering practices/procedures are utilized.**

The extent to which the banks surveyed utilized the various evidence gathering practices below in table 8. A five point Likert scale was used to measure the extent to which the practices are used in evidence gathering. The scale was 1=Not practice, 2=Least practiced, 3=Moderately practiced, 4=Practiced, 5=Fully practiced.

**Table8: Extent to which evidence gathering practices/procedures are used**

Practice/Procedure	Ranking According To Std. Deviation	Mean	Std. Deviation
Observing basic rules of evidence i.e. admissibility, authenticity, completeness, reliable and believable	1	3.900	0.7559
Procedures involving identification preservation analysis and presentation of evidence	2	3.931	0.7527
Observation of the various dos and don'ts in evidence gathering	3	3.8621	0.9534
Procedures of finding relevant evidence from volumes of found evidence	4	3.8276	1.0025
Procedure of removing external avenues of changing the evidence	5	3.8276	1.1973
Documented procedures of collecting the evidence once found and documenting the evidence	6	3.7931	1.0481
Procedure for creating order of volatility -determining the best order of evidence gathering	7	3.7586	1.7863
Procedures of controlling contamination of the collected evidence	8	3.7241	1.0315
Review of applications programs for proper working during relevant period including logs fault records etc was done.	9	3.7931	1.04810
Review of applications programs for proper working during relevant period including logs fault records etc was done.	10	3.7931	1.04810
Procedures of securing collected logs before analysis and thereafter procedures of logging them	11	3.6897	1.9675
Storage media were reviewed and examined	12	3.6897	1.0387
All backup and archived files were reviewed and examined	13	3.6207	1.7752
Suspect computers and systems were examined for proper working during relevant period including service logs fault records etc	14	3.5862	1.0528



A review of access control services was carried out e.g. quality and resilience of facilities (hardware and software identification /authentication services)	15	3.5862	1.8245
Review system/program documentation for: design methods, testing, audit, revisions, and operations and management were carried out.	16	3.5517	1.9851
Identification and examination of audit trails was done	17	3.5172	1.6336
Identification and review of monitoring logs and telecommunication call path tracing was done.	18	3.5172	1.6336
Review and assessment of access control services -quality of security management was done	19	3.4483	1.1828
Review and assessment of encryption methods -resilience and implementation was done	20	3.2759	0.7019
Review and assessment of measuring devices etc and other sources of real evidence including service logs fault records etc was done	21	3.1724	1.1973
Examination of telecommunication devices location of associated activity logs and other records perhaps held by third parties was done	22	3.1379	1.4571
Use of computer programs which provide simulations or animations of events: review of accuracy, reliability and quality was carried out	23	3.000	1.9636
Review system /program documentation of authorized amendments to the information systems was carried out.	24	3.000	1.1952
The incident response plan was followed as a guide to the gathering and collection of the required evidence and the incident response team coordinated the exercise.	25	2.4483	1.2417
A connection to a law enforcement agency was immediate for the delivery of the collected evidence	26	1.5517	0.5061

Ranking of the listed procedures according to their means or standard deviations give the same results, indicating that most of the respondents affirmed that the practices/procedures whose standard deviation rank between 1 and 25 and with a mean score of 3 as shown in table 5 above are used to a moderate extent in gathering evidence.

### 4.6. Challenges of Computer Forensics

The variables collected under this section were used to mainly identify any challenges that exist as the various respondent banks perform the different computer forensics activities.

#### 4.6.1. Level of challenges attached to activities carried out in computer forensics investigation.

The level of challenge to which the banks attach to the various activities carried out in forensic investigation is as shown below in table 9. A five-point scale (Likert scale) was used to measure the level of challenge attached to the various activities in computer forensic investigation. The scale was 1 = not at all challenging, 2 = least challenging, 3 = moderately challenging, 4 = challenging, 5 = extremely challenging.

*Table 9: Challenges attached to activities in computer forensic investigations-*

Challenge	Ranking According to Std. Deviation	Mean	Std. Deviation
Reconstruction of deleted documents without altering the evidence	1	4.0000	.75593
Access to judicial tools by law enforcement agencies for computer based discovery	2	3.9310	.92316
Issuance of preservation order forbidding deletion of email or other computer based information	3	3.8621	.74278
Handling conflict of interests between provisions /requirements of the law and collected evidence	4	3.8621	.69303
Resolving technological incompatibility between storage media and device for restring the media that could have the evidence	5	3.8621	.78940

Preventing permanent destruction of information storage media	6	3.8621	.83342
Getting the code of contract of law enforcement bodies in cases relating to the use of computer evidence	7	3.8276	.75918
Facilitating on site inspection of a party s computer system by an opposing party	8	3.7931	.94034
Apportioning their costs required to retrieve computerized information between the party requesting the information and the respondent	9	3.7586	.95076
Identifying chances of facts being established were damaged	10	3.7241	.70186
Locating and untangling evidence from irrelevant and or privileged records	11	3.7241	.64899
Identifying the best format for the evidence production	12	3.6897	.84951
Apportioning the costs resulting from the format for production (e.g. request to produce in hard copy as well as electronic form)	13	3.6552	1.14255
Finding expert assistance to assist n discovery and retrieval of evidence	14	3.6207	1.11528
Establishing their costs required to retrieve computerize evidence	15	3.5517	.68589
Authentication of collected evidence	16	3.4828	.82897
Determining what evidence to collect first i.e. drawing the order of volatility	17	3.2414	1.09071
Access to sufficient skills in evidence collection preservation and presentation	18	2.6552	.85673
Collecting and handling computer related evidence	19	2.5517	.86957
Evidence analysis and presentation	20	2.2414	.95076

Table 9 above indicates that most of the activities have mean scores of 3 and are ranked between 1 and 17 in terms of standard deviation. Ranking of the statements according to their means or standard deviations in table 9 above show that most of the respondents regard the activities involved in forensic investigation to be moderately challenging.

## 4.7. Section II- Factor Analysis

Factor Analysis was used to uncover relationships amongst the several variables provided for the respondents to select from while responding to the various practices they have adopted as well as the level of challenge they attach to the various activities. The purpose of this procedure was mainly to correlate the numerous variables and condense them into fewer dimensions known as factors. In the context of this research, the variables are the degree of agreement with various specific perception statements while the factors are the general underlying constructs.

### 4.7.1. Extent to which the bank practiced the listed procedures when gathering evidence

The principal axis factoring used extracted five factors. The variables and factors are assumed to be correlated and therefore the sum of squared loadings in table 10 below cannot be added to obtain the total variance. Therefore only the pattern matrix in table 10 below is used for factor analysis.

**Table10: Total Variance Explained**

Factor	Initial Eigen values			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings (a)
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	13.083	52.331	52.331	12.858	51.430	51.430	10.601
2	2.562	10.249	62.580	2.340	9.360	60.791	8.086
3	1.766	7.065	69.645	1.471	5.884	66.675	9.651
4	1.417	5.669	75.314	1.129	4.517	71.192	6.688
5	1.114	4.454	79.768	.824	3.298	74.490	3.173

6	.796	3.184	82.951				
7	.724	2.898	85.849				
8	.690	2.761	88.609				
9	.580	2.318	90.928				
10	.432	1.730	92.658				
11	.363	1.450	94.108				
12	.321	1.285	95.394				
13	.257	1.030	96.423				
14	.211	.845	97.268				
15	.206	.822	98.091				
16	.140	.558	98.649				
17	.094	.377	99.026				
18	.072	.287	99.313				
19	.066	.263	99.575				
20	.044	.176	99.751				
21	.025	.102	99.853				
22	.017	.067	99.920				
23	.013	.052	99.972				
24	.006	.024	99.996				
25	.001	.004	100.000				

**Extraction Method: Principal Axis Factoring.**

**A. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.**

The pattern matrix below in table 11 obtained after doing an oblique rotation shows the loadings for the various factors; five variables explain the total variance of all the variables by up to 74.4%. This is the only pattern needed for interpretation since it is interpretable more than the orthogonal rotation with fewer variables loading significantly on more than one factor (Rummel, 1970). The minimum acceptable loading for each factor was 0.5.

**Table 11: Pattern matrix 1**

VARIABLES	Factor				
	1	2	3	4	5
Observing basic rules of evidence i.e. admissibility, authenticity, completeness, reliable and believable	.016	.852	-.118	.266	-.007
Procedures involving identification preservation analysis and presentation of evidence	-.362	.773	.313	.281	.095
Observation of the various dos and don'ts evidence gathering	-.013	-.199	.854	.206	-.133
Procedures of finding relevant evidence from volumes of found evidence	.238	.050	.599	.208	-.020
Procedure of removing external avenues of changing the evidence	.636	.390	-.315	.072	-.049
Documented procedures of collecting the evidence once found and documenting the evidence	-.004	.927	.091	-.090	-.115
Procedure for creating order of volatility -determining the best order of evidenced gathering	-.002	.942	-.336	.148	.056
Procedures of controlling contamination of the collected evidence	.294	.389	.299	.057	-.331
Procedures of securing collected logs before analysis and thereafter procedures of logging them	.062	.595	.240	-.360	.132
Storage media were reviewed and examined	.012	.002	-.286	.221	.908
All backup and archived files were reviewed and examined	-.059	-.128	.935	.015	-.163
Suspect computers and systems were examined for proper working during relevant period including service logs fault records etc	.924	-.290	-.004	.151	-.136
A review pf access control services was carried out e.g. quality and resilience of facilities (hardware and software identification /authentication services)	-.030	.294	.291	.467	.060
Review system/program documentation for: Design methods, testing, audit, revisions, and operations and	.038	.052	.201	.489	.225

management was carried out.					
Review of applications programs for proper working during relevant period including logs fault records etc was done.	.315	-.259	.175	.579	.207
Identification and examination of audit trails was done	.064	.150	.512	.167	.280
Identification and review of monitoring logs and telecommunication call path tracing was done.	.380	-.085	.397	.330	.069
Review and assessment of access control services - quality of security management was done	.463	.088	.487	.027	.040
Review and assessment of encryption methods - resilience and implementation was done	.724	-.007	.046	.230	.091
Review and assessment of measuring devices etc and other sources of real evidence including service logs fault records etc was done	.843	-.016	-.012	.082	.050
Examination of telecommunication devices location of associated activity logs and other records perhaps held by third parties was done	.287	.331	-.187	.619	.008
Use of computer programs which provide simulations or animations of events: review of accuracy, reliability and quality was carried out	.575	.097	.025	.204	-.404
Review system /program documentation of authorized amendments to the information systems was carried out.	-.038	.176	.696	-.214	-.170
The incident response plan was followed as a guide to the gathering and collection of the required evidence and the incident response team coordinated the exercise.	.693	.257	.126	-.174	.042
A connection to a law enforcement agency was immediate for the delivery of the collected evidence	.849	.042	-.005	-.143	.309
<b>Extraction Method: Principal Axis Factoring.</b>					
<b>Rotation Method: Promax with Kaiser Normalization.</b>					
<b>1 Rotation converged in 12 iterations.</b>					

The pattern matrix that was obtained after doing an oblique rotation using Promax shows that the variables significantly loaded on the factors were as follows: -

**Factor 1:**

- a) Procedures of removing external avenues of changing the evidence: -63.6%;
- b) Suspect computers and systems were examined for proper working during relevant period including service logs, faults records etc: - 92.5%;
- c) Review and assessment of encryption methods, resilience and implementation was done: -72.4%;
- d) Review and assessment of measuring devices etc and other sources of real evidence including service logs, fault records etc were done: -84.3%;
- e) Use of computer programs which provide simulations or animations of events: review of accuracy reliability and quality was carried out: -57.5%;
- f) Incident response plan was followed as a guide to the gathering and collection the evidence and the exercise was coordinated by the incident response team: - 69.3%; and
- g) A connection to always enforcement agency was immediate for the delivery of the collected evidence: - 84.9%.

**Factor2:**

- a) Observing basic rules of evidence i.e. admissibility authenticity completeness reliable and believable: - 85.2%;
- h) Procedures involving identification, preservation analysis and presentation of evidence – 77.3%;
- i) Documented procedures of collecting the evidence once found and documenting the evidence: -92.7%;
- j) Procedure for creating order of volatility -determining the best order of evidenced gathering: -94.2%; and
- k) Procedures of securing collected logs before analysis and thereafter procedures of logging them: -59.5%.

**Factor3:**

- a) All backup and archived files were reviewed and examined: - 93.5%;
- b) Identification and examination of audit trails was done: - 51.2%; and
- c) Review system /program documentation of authorized amendments to the information systems was carried out: - 69.6%.



**Factor4:**

- a) Review of applications programs during proper working during the relevant period including logs, fault records etc was done: - 57.9%; and
- b) Examination of telecommunications devices location of associated activity logs and other records perhaps held by third parties was done: - 61.9%

**Factor5:**

- a) Storage media were reviewed and examined: - 90.8%.

#### 4.7.2. Level of challenges attached to activities carried out in computer forensics investigation.

Like in the previous factor analysis explained above, the principal axis factoring was used and five factors were extracted. Since the variables and factors are assumed to be correlated the sum of squared loadings as shown in table 12 below cannot be added to obtain the total variance. Therefore, only the pattern matrix in table13 is used for factor analysis.

**Table12: Total Variance Explained**

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings(a)
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	9.730	48.651	48.651	9.518	47.590	47.590	7.505
2	2.359	11.797	60.448	2.117	10.583	58.172	8.167
3	1.889	9.446	69.894	1.667	8.334	66.507	4.641
4	1.396	6.981	76.875	1.066	5.329	71.835	4.713
5	1.088	5.439	82.315	.864	4.321	76.157	4.485
6	.663	3.313	85.628				
7	.633	3.165	88.792				
8	.443	2.217	91.009				
9	.411	2.053	93.062				
10	.340	1.702	94.764				
11	.282	1.410	96.175				
12	.199	.995	97.170				
13	.152	.762	97.932				
14	.123	.614	98.546				
15	.112	.561	99.107				
16	.074	.369	99.476				

17	.052	.262	99.737			
18	.024	.120	99.858			
19	.018	.089	99.947			
20	.011	.053	100.000			

**Extraction Method: Principal Axis Factoring.**

**A. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.**

**Table13: Pattern Matrix (1)**

	Factor				
	1	2	3	4	5
Collecting and handling computer related evidence	-.086	-.231	.102	1.105	-.108
Identifying chances of facts being established were damaged	-.025	-.140	.203	-.056	.741
Issuance of preservation order forbidding deletion of email or other computer based information	-.220	1.131	-.056	-.266	.034
Evidence analysis and presentation	-.019	.116	-.134	.815	.086
Access to sufficient skills in evidence collection preservation and presentation	-.017	.109	-.167	.015	.865
Getting the code of contract of law enforcement bodies in cases relating to the use of computer evidence	-.386	.385	.658	.048	-.080
Locating and untangling evidence from irrelevant and or privileged records	-.013	.428	-.085	.353	.273
Establishing the costs required to retrieve computerize evidence	-.142	.827	.080	.213	-.090
Apportioning the costs required to retrieve computerized information between the party requesting the information and the respondent	.014	.345	.364	-.068	.442
Apportioning the costs resulting from the format for production (e.g. request to produce in hard copy as well as electronic form)	.553	.418	.120	.026	-.030
Finding expert assistance to assist n discovery and retrieval of evidence	.886	-.141	.115	-.019	-.152
Determining what evidence to collect first i.e. drawing the order of volatility	.924	-.486	-.055	.083	.170
Facilitating on site inspection of a party s computer system by an opposing party	.384	.576	.085	-.032	-.053

Reconstruction of deleted documents without altering the evidence	.661	.307	.033	.006	-.005
Handling conflict of interests between provisions /requirements of the law and collected evidence	.576	.396	-.113	.026	.102
Resolving technological incompatibility between storage media and device for restring the media that could have the evidence	.505	.481	.005	.179	-.174
Preventing permanent destruction of information storage media	.936	.053	-.131	-.255	-.010
Identifying the best format for the evidence production	.333	.484	.027	.199	.035
Access to judicial tools by law enforcement agencies for computer based discovery	.164	.050	.859	-.188	-.032
Authentication of collected evidence	.119	-.300	.925	.150	.115
<b>Extraction Method: Principal Axis Factoring.</b>					
<b>Rotation Method: Promax with Kaiser Normalization.</b>					
<b>1 Rotation converged in 7 iterations.</b>					

The pattern matrix that was obtained after doing an oblique rotation using Promax shows that the variables significantly loaded on the factors were as follows:

**Factor1:**

- a) Apportioning the costs resulting from the format for production (e.g. request to produce in hard copy as well as electronic form): - 55.3%;
- b) Finding expert assistance to assist in discovery and retrieval of evidence: - 88.6%;
- c) Determining what evidence to collect first i.e. drawing the order of volatility: - 92.4%;
- d) Reconstruction of deleted documents without altering the evidence: - 66.1%;
- e) Handling conflict of interest between provisions/requirements of the law and collected evidence: - 57.6%;
- f) Resolving technological incompatibility between storage media and device for restoring the media that could have the evidence: - 50.5%; and
- g) Preventing permanent destruction of information storage media: - 93.6%.

**Factor2:**

- a) Establishing the costs required to retrieve computer evidence: - 82.7%; and
- b) Facilitating on site inspection of party's computer system by an opposing party: -57.6%.

**Factor3:**

- a) Getting the code of contract of law enforcement bodies in cases relating to the use of computer evidence: - 65.8%;

- b) Access to judicial tools by the law enforcement agencies for computer based discovery: - 85.9%; and
- c) Authentication of collected evidence: - 92.5%.

**Factor4:**

- a) Evidence analysis and presentation: - 81.5%.

## 2. Discussions

**Factor5:**

- a) Identifying chances of facts being established were damaged: - 74.1%; and
- b) Access to sufficient skills in evidence collection, preservation and presentation: - 86.5%.

### Existence of computer forensics

In the summary statistics the following conclusions can be made regarding the existence of computer forensics within the banking industry: -

#### Use of information technology

Use of information technology in Banks' operations is high. Most of the banks have their systems networked and most of their employees are linked to a central server. Given the high level of information systems deployment in the bank operations, there is every indication that these Information Systems are a major target for computer frauds. Once therefore utilized for frauds crimes, then evidence for supporting such cases in court has to be drawn from the Information systems themselves.

#### Transaction authorization method

Most of the banks use both online and real time method to authorize transactions and a few banks use manual method and batch method. With the obvious departure from the traditional authorization methods where a voucher had to physically be signed by a supervisor to authorize a transaction can be completed to the Online methods, the one conclusion that is drawn is the fact that in cases of disputes on who authorized given transactions then computer evidence becomes an only option. From the findings presented in chapter four, it is clear that most of the banks seem to have moved that direction.

#### Nature of frauds experienced

As to the survey, several frauds have been experienced in the industry, most common are unauthorized release of information (69%), false financial statement (65%), Cheque fraud (57%), false invoicing (52%), and laptop theft (51%). As indicated by the study findings,

# CHAPTER FIVE: SUMMARY AND CONCLUSIONS

## 5.1. Introduction

This section gives a summary of the findings and conclusions guided by the objectives of the study as well as the recommendations.

## 5.2. Discussions

From the research findings as presented in chapter four of this study, several conclusions can be drawn. These are discussed in light of the objectives of the study. Prior to discussing the study findings in relation to the objectives; summary findings on the existence of computer forensics within the banking industry will be presented: -

### 5.2.1. Existence of computer forensics

From the summary statistics the following conclusions can be made regarding the existence of computer forensics within the banking industry: -

#### a) Use of information technology

The use of information technology in Banks' operations is high. Most of the banks have their branches networked and most of their employees are linked to a central server. Given the high level of Information systems deployment in the bank operations, there is every indication that the same Information Systems are a major target for computer frauds. Once therefore utilized to perpetuate crime, then evidence for supporting such cases in court has to be drawn from the Information systems themselves.

#### b) Transaction authorization method

Majority of the banks use both online and real time method to authorize transactions and a small percentage use manual method and batch method. With the obvious departure from the manual authorization methods where a voucher had to physically be signed by a supervisor before a transaction can be completed to the Online methods, the one conclusion that is drawn here is the fact that in cases of disputes on who authorized given transactions then computer forensic evidence becomes an only option. From the findings presented in chapter four, majority of the banks seem to have moved that direction.

#### c) Nature of frauds experienced

According to the survey, several frauds have been experienced in the industry, most common are: - Unauthorized misuse of information (69%), false financial statement (65%), Cheque forgery (57%), false invoicing (52%), and laptop theft (51%). As indicated by the study findings,

those perpetuated through Information Systems account for the highest %, which therefore implies that, any evidence has to be collected from the Information Systems.

#### **d) Ways the frauds were mainly discovered**

The survey revealed that frauds in the industry were mainly discovered through:- third party Investigations, external auditor review, employee's investigation, notification by customer, internal auditor review and anonymous letter/informant.

#### **e) Use of computer evidence**

Most banks are still not utilizing Computer evidence despite the heavy deployment of computers in their operations. It is however essential to note that though computer forensics evidence is a fairly new concept, the percentage of banks using evidence drawn from computers is steadily growing. Where banks are using computer evidence real evidence (logs production) was quoted as the main type of evidence used to support litigation. Other methods are still to be explored.

In conclusion therefore; the statistics obtained provide every indication that computer forensic evidence indeed exists within the Banking industry. Although the percentage of the Banks utilizing it for support of litigation is slightly lower than those not using it, other factors other than its existence may be contributing to the above trend.

### **5.2.2. Summary discussions in light of the study objectives**

This study had two main objectives namely: -

- i.) Determine the extent of adoption of computer forensics practices in litigation support within the banking industry in Kenya; and
- i.) To identify the challenges faced by the banking industry in Kenya while collecting and using computer evidence for litigation support.

The literature reviewed presented a number of practices that are expected to be performed when dealing with computer evidence. It further presented a number of challenges commonly experienced when working computer evidence. This section will present the conclusions drawn from the results earlier presented in Chapter four in line with the study objectives.

**a) To determine the extent of adoption of computer forensics practices in litigation support within the banking industry in Kenya.**

According to summary statistics, all the banks consider the Procedures involving identification, preservation analysis and presentation of evidence (mean score=3.931) as the most adopted practice in gathering evidence to support litigation. Other practices that have indeed been adopted to a moderate extent include: -

- a) Observing basic rules of evidence i.e. admissibility, authenticity, and completeness, reliable and believable (mean score=3.9.);
- b) Observation of the various dos and don'ts in evidence gathering (mean score= 3.9);
- c) Procedures of finding relevant evidence from volumes of found evidence (mean score=3.8);
- d) Documented procedures of collecting the evidence once found and documenting the evidence (Mean score= (3.5);
- e) Procedure for creating order of volatility -determining the best order of evidence gathering (mean score=(3.5);
- f) Procedures of controlling contamination of the collected evidence (mean score=3.2); and
- g) Procedures of securing collected logs before analysis and thereafter procedures of logging them (mean score=3.0).

The Removal of external avenues from changing the evidence was the least adopted practice by the banks in gathering evidence with a mean score of 2.4 while the use of computer programs, which provide simulations, or animation of events has not been adopted at all. Practices such as following an Incident Response Plan as a guide to the gathering and collection of the required evidence as well as having incident response team to coordinate the exercise that are regarded very crucial in guarding the evidence from bias do not seem to have been adopted to any meaning full levels. The connection to a law enforcement agency for the immediate delivery of the collected evidence has not been adopted to a high level as would have been expected.

Further it can be noted from the summary results presented above that most banks seem to have adopted those practices that may lead to the evidence being altered and paid little or no attention on the other areas relating to computer evidence. The practices not adopted may, therefore, explain why there is a slightly smaller percentage of banks utilizing computer forensics evidence for litigation support despite the heavy deployment of computers hence high numbers of computer crimes being experienced in the banking industry.

**b) To identify the challenges faced by the banking industry in Kenya while collecting and using computer evidence for litigation support.**

The summary statistics indicated that most banks found a number of the activities involved in collecting and using computer evidence to be moderately challenging. The most challenging activity was found to be the reconstruction of deleted documents without altering the evidence (Mean score = 4.0). Other activities found to be moderately challenging were as follows: -

- a) Access to judicial tools by law enforcement agencies for computer based discovery (3.9);
- b) Issuance of preservation order forbidding deletion of email or other computer based information. (3.8);
- c) Handling conflict of interests between provisions /requirements of the law and collected evidence. (3.8);
- d) Resolving technological incompatibility between storage media and device for restring the media that could have the evidence. (3.8);
- e) Preventing permanent destruction of information storage media (3.8);
- f) Getting the code of contract of law enforcement bodies in cases relating to the use of computer evidence. (3.8);
- g) Facilitating on site inspection of a party s computer system by an opposing party (3.7);
- h) Apportioning their costs required to retrieve computerized information between the party requesting the information and the respondent (3.7);
- i) Identifying chances of facts being established were damaged (3.7);
- j) Locating and untangling evidence from irrelevant and or privileged records (3.7);
- k) Identifying the best format for the evidence production (3.6);
- l) Apportioning the costs resulting from the format for production (e.g. request to produce in hard copy as well as electronic form)(3.6);
- m) Finding expert assistance to assist in discovery and retrieval of evidence (3.6);
- n) Establishing their costs required to retrieve computerize evidence (3.5);
- o) Authentication of collected evidence (3.4); and
- p) Determining what evidence to collect first i.e. drawing the order of volatility (3.2).

The discipline of computer forensic is fairly new not only to the banking industry in Kenya but also to nearly all sectors worldwide. While computer crimes continue to increase day by day, various guidelines relating to the evidence drawn from the computers where the crimes are executed remain very gray. This coupled with the limitation in training on the subject for the law enforcement agents as well the a clear legal framework of how computer evidence should be treated presents numerous challenges to nearly all the activities related to the identification and utilization of computer evidence for litigation support as supported by the above responses received from the banks that responded.



### 5.2.3. Factor Analysis Discussions

The results presented in the previous section though provide an indication of which activities have been adopted as well as a list of activities identified as most challenging as far as computer forensics is related, they do not present precisely the list of top most adopted practices as well top in the list of challenges experienced. This factor analysis section is aimed at discussing the research findings in light of the study objectives more precisely.

#### a) Extent to which the banks practiced various procedures when gathering evidence

Turning to the results depicted in the pattern matrices of Table 8; the following discussions emerge. That there are indeed five main computer forensics practices that have been adopted to a large extent as indicated by the procedures practiced by the banking industry in gathering of computer evidence for litigation support. The five factors extracted via a factor analysis that represent the various practices in table 8 can be identified as follows:-

##### i.) Factor 1: - Determination of Legal right

Of the 25 practices related to gathering of computer evidence, 6 loaded heavily (between 69.3% and 92.5%) under factor 1. The mentioned practices rotate under the determination of legal right for the evidence hence factor 1 was named Determination of Legal right. The 5 practices loaded as follows; 92.5% of the respondents cited the inspection of suspect computers and systems to ascertain their working status prior to the compromise as the key activity performed. Connection to a law enforcement agency for the immediate delivery of collected evidence -84.9%; Review and assessment of measuring devices and other sources of real evidence- 84.3%; The review and assessment of encryption methods and resilience- 84.9% and use of the incident response plan as a guide to the gathering and collection of the evidence as well as having the exercise coordinated by the incident response team- 69.3%. It is important to note that all the above practices are aimed at ensuring that the evidence gathering will finally meet the basic rules and once gathered it will not be nullified. Despite the absence of a proper legal framework on the handling of evidence from computers; it can be noted that the banking industry has moved to adopt various practices as indicated above to ensure the evidence they gather meets all the legal requirements.

##### ii.) Factor2: -Gathering evidence

Under factor 2, 5 practices loaded heavily with loadings of 59.5% to 94.2%. The procedures related to creating order of volatility -determining the best order of evidence gathering loaded at 94.2% implying that it is the most adopted procedure in as far as gathering of evidence is concerned. Others that loaded heavily under factor 2 include: - Documented procedures of

collecting the evidence once found and documenting the evidence: - 92.7%; Observing basic rules of evidence i.e. admissibility, authenticity, completeness, reliable and believable –85.2%; Procedures involving identification, preservation analysis and presentation of evidence – 77.3%; Procedures of securing collected logs before analysis and thereafter procedures of logging them –59.5%.

From earlier statistics presented elsewhere in this study, the banking industry is heavily dependent on computers/Information Systems for their daily operations. The chances of computer crimes being committed are therefore high, explaining the need by various banks to adopt relevant practices related to the gathering of computer evidence as depicted by the above practices under factor 2.

### iii.) Factor 3: - Analysis

Three practices loaded heavily under factor 3. The review and examination of backups and archived files loaded highest at 93.5% giving an indication that the practice was highly adopted by the banks that responded. Other practices were: - review of system /program documentation for authorized amendments to the Information Systems loading at 69.6% and the Identification and examination of audit trails at 51.2%. All three practices form part of the various variables under analysis that a computer forensic scientist should consider when evaluating a system under investigation as earlier indicated in the literature review.

### iv.) Factor4: - Correlation of Events

Computer file dates and times can be extremely important as evidence; the establishment of Timeline and ability to correlate events and do a reconstruction are therefore critical practices in any computer investigation process. From the survey, respondent banks picked on two practices that relate to the correlation of events once a computer crime has been committed. The 2 loaded heavily under factor 4 hence the reason for factor 4 being named Correlation of Events. Examination of telecommunications devices; location of associated activity logs and other records loaded at 61.9% while the review and examination of backups; applications programs during proper working during the relevant period including logs, fault records etc was done loaded at 57.9%. The statistics therefore imply that the banking industry has adopted relevant practices that can help in establishing a particular time when an incident occurred as well as the media involved hence enabling the computer forensic investigators correlate incidents with forensic findings to prove or disprove a theory

#### v.) Factor 5: - Backup Procedures

Storage media were reviewed and examined is the only practice that loaded heavily under factor 5 with a loading of 90.8%. It relates to any procedure/practices performed to offer guarantees that the internal drives remain intact and no processes access it hence evidence is protected.

#### Summary

The statistics presented by the factor analysis strongly indicate adoption of the various practices/ procedures performed during the Computer Forensics Process Methodology steps earlier identified in the Literature review, a good percentage of the methodology has been adopted giving a total of 5 steps in the process methodology that have been adopted and are being applied through various practices by the Kenyan banking industry. It is essential to however note that practices related to 2 of the 7 steps have not been adopted at all and this relate to the Seize of the Computer System and Evidence as well as those related to presentation of the evidence.

The lack of adoption of the 2 practices and hence failure to perform the 2 related steps could imply that though the banking industry has done as much to get evidence from computer systems, the same is still not fully recognized in the Kenyan legal setup. In such a case therefore judges may not wish to know if the records are reliable i.e. if the computers involved were segregated after the crime and how the evidence was handled up to the point of presenting it to the courtroom.

#### b) Level of challenge attached to activities carried out in computer forensics investigation.

From the analysis in table6, five factors were extracted via the factor analysis as depicted in the pattern matrix in table 9. The 5 factors are tied to various activities carried out in computer forensics investigations and can therefore be considered as the major challenges experienced by the Banking industry in utilizing computer evidence for litigation support. The five key factors identified, as main challenges were follows: -

#### i.) Factor1: - Identification & Collection of evidence as well as the forms of production for computer evidence

Potentially discoverable records that may contain computer evidence are stored according to computer logic, as opposed to "business-record" logic, this can make computer evidence difficult to locate and untangle from irrelevant and privileged records. This proposition was confirmed by the survey results in which a number of activities related to the identification,

collection as well as the form of production of evidence after collection loaded heavily under factor 1 hence named Identification & Collection of evidence as well as the forms of production for computer evidence. The activities in question all relate to the processes of identification, gathering and collection of computer evidence and include: - Preventing permanent destruction of information storage media loaded highest at 93.6%; determining what evidence to collect first i.e. drawing the order of volatility at 92.4%; finding expert assistance to assist in discovery and retrieval of evidence loaded at 88.6% while reconstruction of deleted documents without altering the evidence loaded 66.1%.

The activities above selected by the respondent banks imply that the banking industry in Kenya though may have potentially relevant data in the various locations whether in each employee desktop computer, disks or other removable data storage media, a laptop computer, and a hand-held personal organizer or in network servers; they are still faced with the challenges related to the retrieval of that same evidence.

#### **ii.) Factor 2: - On-site inspection and related costs**

Two of the twenty activities performed in a Computer Forensic investigation loaded heavily under factor 2. The two relate to On-site Inspection and the cost implications since during an inspection there is business disruption as a view of the computer system is being done. Establishing the costs required while retrieving the computer evidence loaded highest at 82.7% while facilitating the On-site inspection of affected party's computer system by an opposing party loaded at 57.6%. Given the sensitivity of the data held by banks, the indication here would be that banks experience difficulties or find it virtually impossible to protect privileged information at times where they may be requested for an On-site inspection. Further where they overcome such other difficulties the costs involved and how to apportion them after an On-site inspection remains challenging.

#### **iii.) Factor 3: - Access to computer forensics guidelines**

Access and collection of electronic evidence raises unique issues that normally do not occur or are less problematic in conventional, paper-based; an incident response plan therefore becomes useful in providing relevant guidelines to guide discovery and collection of computer evidence. A number of activities selected by the various banks as challenging are related to access to computer forensics guidelines and loaded heavily under factor 3 hence the reason for the factor being named Access to computer forensics guidelines. Authentication of collected evidence loaded highest at 92.5%; Access to judicial tools by the law enforcement agencies for computer based discovery loaded at 85.9% and getting the code of contract of law enforcement bodies in cases relating to the use of computer evidence loaded at 65.8%.

## 3.3 Conclusions

From the above results; it can be concluded that though the banking industry is faced with various computer threats given their level of computer use in the day-to-day operations, the relevant capacity to carry out computer forensics work may be inadequate or completely missing.

### iv.) Factor4: - Analysis & presentation of computer evidence

One of the various computer forensics activities loaded heavily under factor 4. Evidence analysis and presentation activity loaded at 81.5% under factor 4. Computer evidence as discussed elsewhere in this survey could be voluminous and isolating potential evidence from large volumes of available data for analysis can be challenging. If a crime is committed via e-mail for example; the sheer volume which can be staggering, even for a small company or individual and its lack of a coherent filing system can offer various challenges to the investigators. This activity is further complicated by the need to have evidence processed safely, any discrepancies eliminated and the evidence safely retrieved for analysis. From the survey results, the banking industry in Kenya is still experiencing the challenges faced elsewhere in as far as the Analysis and presentation of computer evidence is concerned.

### v.) Factor 5: - Access to expert assistance

Two of the twenty listed computer forensics activities loaded heavily under factor five. The Access to sufficient skills in evidence collection, preservation and presentation loaded highest at 86.5% while Identifying chances of facts being established were damaged loaded at 74.1%. The two activities were named access to expert assistance. Expert assistance is necessary for the assessment of computer systems involved crimes and for negotiating the technical aspects of conducting discovery, including search protocols, privilege and relevance screening, and production with the relevant parties among other duties. Where access to expert assistance is an issue, then legal difficulty is likely to be faced by the party seeking to redress cyber-crime in the court using digitally based evidence since its chances of acceptability are low. The Kenyan banking sector is not an exception hence given the survey results, the sector could be experiencing legal difficulty while using electronic evidence explaining why a slightly higher percentage of banks indicated in earlier sections they had not used computer evidence as much in litigation support than those who used it.

### 5.3. Conclusions

The main aim of this survey was to identify the extent to which various computer forensics practices have been adopted in litigation support within the banking industry in Kenya and the challenges faced by the banking industry in Kenya while collecting and using computer evidence for litigation support. The survey revealed that computer evidence indeed exists within the Banking industry and is widely being applied for litigation support. Though various forms of evidence have not been used by the Banking industry, some forms of evidence such as real evidence (retrieved logs) has been used much by the banks to support litigation.

From the survey, five main practices/procedures were identified as having been largely adopted in gathering forensic evidence for litigation support. They include: -

- i.) Determination of legal right;
- ii.) Gathering of evidence;
- iii.) Analysis of gathered evidence;
- iv.) Correlation of evidence to events that occurred; and
- v.) Backup procedures

From the above activities identified as having been largely adopted; it can therefore be concluded that the Computer Forensic Science Investigation process discussed earlier in the literature review section that has been widely adopted elsewhere in the world has been adopted by the banking industry in Kenya. The process outlines seven steps aimed at ensuring that evidence is processed safely and discrepancies are eliminated as electronic evidence is retrieved for analysis. Out of the 7 steps, 5 are represented in the practices identified above as the largely adopted during computer forensic exercises within the banking industry.

Further five main activities (grouped set of activities) were identified as the most challenging when the banking industry in Kenya is collecting and using computer evidence for litigation support. The five were identified as: -

- i.) Identification & collection of evidence as well as the forms of production for computer evidence;
- ii.) On-site inspection of information systems and related costs;
- iii.) Access to computer forensics guidelines to guide the computer forensics investigations process methodology;
- iv.) Analysis & presentation of computer evidence; and
- v.) Access to expert assistance for provision of assistance in the handling and presentation of computer evidence.

## **5.4. Limitations of the Study & Suggestions for Further Research**

This part of the study discusses the limitations of the study and includes suggestions for further research.

### **5.4.1. Limitations**

The limitations of the study can be summarized as below:

#### **a) Geographical scope**

All the respondents were drawn from Nairobi. For more accurate conclusions, a larger study population with a wider geographical scope would have been better.

#### **b) Financial Resources**

Limited finances and time constraints limited the number of respondents picked in each Bank and hence the scope of the study.

#### **c) Failed responses**

Any information held by the Banking industry is highly confidential and therefore not easily accessible. With the study targeting information related to System security, most banks completely declined to respond to the questionnaire despite the assurances given that the collected data will be treated confidentially.

#### **d) Related studies locally**

There are no locally known studies on computer forensics and in addition the concept was fairly new to the respondents. Generally the area of Information Security is still being setup in most banks and some banks were not willing to give any information simply to avoid being considered laggards in the area. Additionally the review of literature heavily relied on studies carried elsewhere to have deductions made for the local scene.

## 5.4. Limitations of the Study & Suggestions for Further Research

This part of the study discusses the limitations of the study and includes suggestions for further research.

### 5.4.1. Limitations

The limitations of the study can be summarized as below:

#### a) Geographical scope

All the respondents were drawn from Nairobi. For more accurate conclusions, a larger study population with a wider geographical scope would have been better.

#### b) Financial Resources

Limited finances and time constraints limited the number of respondents picked in each Bank and hence the scope of the study.

#### c) Failed responses

Any information held by the Banking industry is highly confidential and therefore not easily accessible. With the study targeting information related to System security, most banks completely declined to respond to the questionnaire despite the assurances given that the collected data will be treated confidentially.

#### d) Related studies locally

There are no locally known studies on computer forensics and in addition the concept was fairly new to the respondents. Generally the area of Information Security is still being setup in most banks and some banks were not willing to give any information simply to avoid being considered laggards in the area. Additionally the review of literature heavily relied on studies carried elsewhere to have deductions made for the local scene.



## 5.4.2. Suggestions for further research

The area of Computer Forensics is fairly new not only to the Banking Industry in Kenya but also to all other sectors in most parts of the world. The books and articles written on computer forensics and the use of electronic evidence for litigation are based on the West mainly the United States of America and the United Kingdom where levels of computer/ information systems application in day-to-day operations is high and the law enforcement agencies are fully developed.

Available: [http://www.scmagazine.com/scmagazine/2001\\_04/cover/cover.html](http://www.scmagazine.com/scmagazine/2001_04/cover/cover.html)

Computer Forensics as a discipline and its application therefore need to be explored further in Kenya and clear policies stipulated both at national and sector levels in order to ensure: -

- i.) Practices/procedures such as the proper collection and preservation of original evidence in its entirety performed during computer forensics investigations comply with legal requirements;
- ii.) The evidence collected after a system compromise is admissible in court; and
- iii.) Relevant training is offered to the computer forensics investigators; the expert witnesses as well as all the law enforcement agents for justice to be done in cases where computers/information systems were used to perpetuate a crime.

Available: [www.cdf.org](http://www.cdf.org), (2001).

Central Bank of Kenya. (2003) "Bank Supervision Annual Report" Retrieved from Worldwide Web on July 10, 2004.

Central Bank of Kenya. (June, 2004) "Kenya Economic Review" Retrieved from Worldwide Web on July 16, 2004.

Seppel, M. (2001), "Computer Forensics and Litigation Support," Technical Paper, Computer Forensic Consultants Ltd.

Stallnick, William R. & Belloni, Steven M. (1994). Firewalls and Internet Security. Reading, Masson Wesley, NY.

CommerceNet Research Council. (2000). "Industry Statistics", Retrieved August 10, 2003 from World Wide Web. Available: <http://www.commerce.net/research/stats/wwwstats.html>

Cooper, D. R. & Emery, C. W. (1998). Research methods. Homewood, IL: Richard D. Irwin, Inc.

Webzchronicle.com, (2007). "Computer Crimes Pose Severe Threats Toward U.S. and Western Countries", Retrieved from the World Wide Web on August 10, 2004. Available: <http://webzchronicle.com/background01/jul/usasiathreat.htm>

Whelan, Joan and Rodger, Kolin (2001). "Electronic Discovery of computer-based evidence", Retrieved from the World Wide Web on August 1, 2004. Available: <http://www.forensics.com/resources/evid.htm>

Forensic Science Communications. (2000). "Recovering and Examining

## REFERENCES

- American Bar Association, Section of Science and Technology, "Guide to the Prosecution of Telecommunication Fraud by the Use of Computer Crime Statutes", Proceedings of the American Bar Association, 1989.
- Armstrong, I., (2001). "Computer Forensics, Tracking Down the Clues". Retrieved from the World Wide Web on July 28, 2003.  
Available: [http://www.scmagazine.com/scmagazine/2001\\_04/cover/cover.html](http://www.scmagazine.com/scmagazine/2001_04/cover/cover.html)
- Anderson, M, (2000), "Identifying Internet Activity", Retrieved from the World Wide Web on August 1, 2004.  
Available: <http://www.forensics-intl.com/artipfl.html>
- Betts, Bill. (2000). "Crime Scene Information Security Magazine". Retrieved from the World Wide Web on July 30, 2003.  
Available: <http://www.nlectc.org/inthenew/crimeseen.html>
- British Telecommunications Ignite Solutions. (2001). "The Art of Being Prepared". Retrieved from the World Wide Web on August 10, 2004.  
Available: <http://www.btignitesolutions.com/insights/articles/beingprepared.htm>
- CERT Coordination Center. "How the FBI Investigates Computer Crime."  
Available: [www.cert.org](http://www.cert.org), (2001).
- Central Bank of Kenya. (2003) "Bank Supervision Annual Report" Retrieved from Worldwide Web on July 10, 2004.
- Central Bank of Kenya. (June, 2004) "Kenya Economic Review" Retrieved from Worldwide Web on July 15, 2004.
- Chappell, M. (2001), "Computer Forensics and Litigation Support," Technical Paper, Computer Forensic Consultants Ltd
- Cheswick, William R. & Bellovin, Steven M. (1994). Firewalls and Internet Security. Reading: Addison Wesley. NY.
- CommerceNet Research Council. (2000). "Industry Statistics". Retrieved August 10, 2003 from the World Wide Web. Available: <http://www.commerce.net/research/stats/wwstats.html>
- Cooper, D. R. & Emory, C. W. (1998). Research methods. Homewood, IL: Richard D. Irwin, Inc.
- EBizChronicle.com. (2001). "Computer Crimes Pose Severe Threats Toward U.S. and Western Businesses". Retrieved from the World Wide Web on August 10, 2004. Available: <http://ebizchronicle.com/backgrounders01/jul/russiathreat.htm>
- Feldman, Joan and Rodger, Kohn (2001). "Electronic Discovery of computer-based evidence". Retrieved from the World Wide Web on August 1, 2004. Available: <http://www.forensics.com/resources/evic.htm>
- Forensic Science Communications. (2000). "Recovering and Examining

Computer Forensic Evidence". Retrieved July 20, 2004 from the World Wide Web. Available: <http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm#Computer%20Forensic%20Science>

Gilmore, (2001). "A Recap and Review of "Cybercrime—Supporting Cyber Sleuths". [Review of the article, Cybercrime—Supporting Cyber Sleuths]. Retrieved August 12, 2001 from the World Wide Web. Available: <http://karenorobinson.tripod.com/recapreview.doc>

INFOCOMM security, (2002) "Country Report on Singapore: Asia-Pacific Conference on Cybercrime and Information Security" Seoul, Republic of Korea, 11-13 November.

Isner, Jonathan, D.(2003) "Computer Forensics: An Emerging Practice in the Battle against Cyber Crime", SANS Institute.

Kroll Ontrack, "Kroll Ontrack Cyber Crime and Computer Forensics News". Cyber Crime and Computer Forensics News, Volume 1, Number 9 (October 2003).

McKemmish, R, (1999) "What is Forensic Computing?" Australian Institute of Criminology Report, June 1999, Available at: <http://www.aic.gov.au/publications/tandi/ti118.pdf>

McPeak, K. et al (2001), "Computer Forensic Science: A methodology", Proceedings of the International Conference on E-Commerce Security, PP 754-776.

Muiruri, Stephen, "CBK staff implicated in fraud". Daily Nation, Friday, November 19, 1999  
Muiruri, Stephen, "Police alarmed by rise in cyber fraud". Daily Nation, February 18, 2004

Jacque, Kerubo, "Protect Innocent depositors from losses". Daily Nation, March 26, 2004

New Technologies. (2001). "Computer Investigations Defined". Retrieved from the World Wide Web on August 11, 2004. Available: <http://www.forensics-intl.com/def5.html>

New Technologies. (2001). "Unallocated File Space Defined". Retrieved from the World Wide Web on August 18, 2004.  
Available: <http://www.forensics-intl.com/def8.html>

Njogu, w, "A survey of the Extent of ICT Adoption among Parastatals", Unpublished MBA Project, University of Nairobi, 2004.

Noblett, et al. (2000 October). "Recovering and Examining Computer Forensic Evidence." Forensic Science Communications, Retrieved from the World Wide Web on September 2004. Available: <http://www.fbi.gov>.

Nyambati, R, "Information Technology Planning Practices: The Case of Banking Sector", Unpublished MBA Project, University of Nairobi, 2001

Roe, Alan, R. "Key Issues in the Future Development of Kenyan Banking" Paper to Stakeholders' Forum on Financial Sector Reforms Mombasa, 15th to 17th April, 2004.

Rubinstein, Bruce., "Electronic Discovery Costs are Leveraging Settlements" Corporate Legal Times, September, 1997.

Rummel, R.J. (1970). Applied Factor Analysis. Evanston: Northwestern University Press

Saita, A (2001). "Resources to Secure Your Business Enterprise". Information Security Magazine, May, Volume 124.

Shipley, T (2001), "Cyber crime: Supporting Cyber Sleuths". Retrieved from the World Wide Web on July 23, 2004. Available: [http://www.infosecmag.com/articles/july01/features\\_cybercrime.shtml](http://www.infosecmag.com/articles/july01/features_cybercrime.shtml)

Sommer, P., (1997), "Computer Forensics: An Introduction", Retrieved from the World Wide Web on August 18, 2004, Available: <http://www.virtualcity.co.uk/vcaforens.htm>

Summer, R., (1997). *Secure Computing*. New York: McGraw Hill. P. 166.

United States Department of Justice, Computer Crime and Intellectual Property Section (2001), "Federal Computer Intrusion Laws", Retrieved from the World Wide Web on July 28, 2004. Available: <http://www.cybercrime.gov/cclaws.html>

US Naval Observatory, (2001), "Time Service Department", Retrieved from the World Wide Web on August 12, 2004, Available: <http://tycho.usno.navy.mil/time.html>

Villano, M. (2001, March 1). CIO Magazine. "I.T. Autopsy." Available: [www.cio.com](http://www.cio.com)

Wack, J. P. (November, 1991). "Establishing a Computer Security Incident Response Capability", Retrieved from the World Wide Web on July 27, 2004. Available: <http://csrc.ncsl.nist.gov/publications/nistpubs/800-3/800-3.pdf>

Walker, D. (2001), "Computer Forensics: Techniques for Catching the 'perp' protect company data", Retrieved from the World Wide Web on July 31, 2004. Available: <http://www.serverworldmagazine.com/monthly/2001/03/forensics.shtml>

Willhite, Sarah A, (2002) "Computer Forensics" Available in the Worldwide Web

Witter, F. (2001, April 20) "Legal Aspects of Collecting and Preserving Computer Forensic Evidence." Information Security Reading Room, Available: [www.sans.org](http://www.sans.org)

Wright, B., (1996), "The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues, published by the Computer Law Association", Retrieved from the World Wide Web on August 10, 2004. Available: <http://www.cla.org/RuhBook/chp7.htm#fn8>

Wright, T., (2001). "An Introduction to the Field Guide for Investigating Computer Crime - Part 1", Available: <http://www.securityfocus.com/frames/?focus=ih&content=/focus/ih/articles/crimeguide1.html>

# APPENDICES

## Appendix 1: Letter of Introduction

\*\*\*\*\*

**ANNEROSE N. NGEMU,  
UNIVERSITY OF NAIROBI,  
FACULTY OF COMMERCE,  
DEPARTMENT OF MANAGEMENT SCIENCE,  
P.O. BOX 30197,  
NAIROBI.**

Dear respondent,  
I am a postgraduate student in the Faculty of commerce, University of Nairobi, pursuing a Masters in Business Administration degree programme. I am undertaking a Management research project on: - ***A survey of Computer Forensics practices in litigation support: The case of the banking industry in Kenya.***

You have been selected as one of the respondents. I therefore request you to fill the attached questionnaire to the best of your knowledge. The information from the questionnaire is needed purely for academic research purposes and will therefore be treated with strict confidence. In no way will your name or the name of your bank appear in the final report.

A copy of the final report will be made available to you upon request. Thank you for your valuable cooperation.

Yours faithfully,

**A.N. Ngemu**  
**MBA STUDENT**

## Appendix 2: Questionnaire

\*\*\*\*\*

### Part I

- 1) Ownership of Bank
  - Foreign owned
  - Locally owned
  - Partially Foreign, partially locally owned
- 2) Customer base ('000) (Please tick)
  - Less than 10
  - Between 10 and 50
  - Between 50 and 100
  - More than 100
- 3) Number of branches
  - Less than 5
  - Between 5 and 20
  - Between 21 and 100
  - More than 100
- 4) What is the level of Information Technology utilizations in the Bank's operations?
  - High
  - Medium
  - Low

\*\*\*\*\*

### Part II

- 5) Are the Bank branches selected in part I above electronically linked to a central server?
  - Yes
  - No
- 6) How many members of staff can currently connect to the central server?
  - All
  - Three quarters
  - Half
  - Quarter
  - None
- 7) Among the listed transaction authorization methods, which one is your Bank using?
  - Manual authorization
  - Batch authorization
  - Online not real-time
  - Online and real-time

10) Among the different kind of frauds listed below, please tick those that have been experienced by your Bank.

- Others, Please specify-----
- Corporate espionage
- Active wiretap
- Credit card fraud
- False financial statements
- Hacking for financial/transactional fraud
- Purchase for personal use
- Cheque forgery
- Unauthorized/misuse of information
- Electronic and telecomm fraud
- False invoicing
- Secret commission/bribery
- System penetration (e.g. web defacement)
- Laptop theft
- Denial of service
- Insider abuse of Information Systems
- Misuse of General ledger accounts
- Theft of proprietary information
- Others, Please specify-----

9) How was the fraud discovered?

		NP	LP	MP	P	FP
1	<input type="checkbox"/> Third party investigation					
	<input type="checkbox"/> External auditor review					
2	<input type="checkbox"/> Employee investigation					
	<input type="checkbox"/> Notification by supplier					
3	<input type="checkbox"/> Others/notification by authority					
	<input type="checkbox"/> Notification by customer					
4	<input type="checkbox"/> Internal auditor review					
	<input type="checkbox"/> By chance					
5	<input type="checkbox"/> Internal controls					
	<input type="checkbox"/> Anonymous letter/informant					
6	<input type="checkbox"/> Management investigation					
	<input type="checkbox"/> Others, Please specify-----					
7	Procedure for creating order of Volatility- determining the best order of evidence gathering					

10) Among the frauds selected above, has the Bank been involved in a case(s)/fraud where computer evidence was to be retrieved for support of litigation?

- Yes
- No

If yes, then please answer the rest of the questions in this part.

11) Among the following types of computer evidence; which one was employed for the above case(s)

- Real evidence (Logs produced)
- Testimonial (evidence supplied by a forensic expert)
- Hearsay (evidence supplied by a person who was not a direct witness)
- Real and Testimonial
- Real; testimonial and Hearsay

12) In gathering the above evidence, one would expect various practices involving evidence gathering to have been performed. Please indicate the extent to which the bank practiced the listed procedures when gathering evidence. (Place a tick in the column of your answer of each practice. Ratings are from Fully practiced to least practiced)

- Fully Practiced (FP)..... 5
- Practiced (P).....4
- Moderately Practiced (MP).....3
- Least Practiced (LP).....2
- Not Practiced (NP).....1

S/N	Practice	NP	LP	MP	P	FP
1	Observing basic rules of evidence i.e. admissibility, authenticity, completeness, reliability and believable.					
2	Procedures involving identification; preservation; analysis and presentation of evidence.					
3	Observation of the various dos and don'ts of evidence gathering					
4	Procedures of finding relevant evidence from volumes of found evidence					
5	Procedure of removing external avenues of changing the evidence					
6	Documented procedures of collecting the evidence once found and documenting the evidence					
7	Procedure for creating order of Volatility- determining the best order of evidence gathering.					



8	Procedures of controlling contamination of the collected evidence.					
9	Procedures of securing collected logs before analysis and thereafter procedures of logging them.					
10	Storage media were reviewed and examined					
11	All back-up and archived files were reviewed and examined					
12	Suspect computers and systems were examined for "proper" working during relevant period, including service logs, fault records, etc.					
13	A review of access control services was carried out e.g. - quality and resilience of facilities (hardware and software, identification /authentication services)					
14	Review of system / program documentation for: design methods, testing, audit, revisions, and operations management was carried out.					
15	Review of applications programs for "proper" working during relevant period, including logs, fault records, etc was done.					
16	Identification and examination of audit trails was done					
17	Identification and review of monitoring logs & Telecommunication call path tracing was done.					
18	Review and assessment of access control services - quality of security management was done					
19	Review and assessment of encryption methods - resilience and implementation was done					
20	Review and assessment of measuring devices, etc. and other sources of real evidence, including service logs, fault records, etc. was done					
21	Examination of telecommunication devices, location of associated activity logs and other records perhaps held by third parties was done					
22	Use of computer programs which provide simulations or animations of events: review of accuracy, reliability and quality was carried out.					
23	Review of system / program documentation of					

	authorized amendments to the Information System was carried out					
24	The Incident response plan was followed as a guide to the gathering and collection of the required evidence and the exercise was coordinated by the Incident Response Team.					
25	A connection to a Law enforcement agency was immediate for the delivery of the collected evidence.					

13) Using the scale below, indicate the level of challenge the bank attaches to the listed activities that have to be carried out in the process of a computer forensics investigation:-

Extremely Challenging (EC).....5

Challenging (C).....4

Moderately Challenging (MC).....3

Least Challenging (LC).....2

Not at all Challenging (NC).....1

S/N	Activity	NC	LC	MC	C	EC
1	Collecting and handling computer related evidence					
2	Identifying chances of facts being established were damaged					
3	Issuance of preservation order forbidding deletion of e-mail or other computer-based information					
4	Evidence analysis and presentation					
5	Access to sufficient skills in evidence collection, preservation & presentation					
6	Getting the code of contact of law enforcement bodies in cases relating to the use of computer evidence.					
7	Locating and untangling evidence from irrelevant and (or) privileged records					
8	Establishing the costs required to retrieve computerized information evidence.					
9	Apportioning the costs required to retrieve					

	computerized information between the party requesting the information and the respondent					
10	Apportioning the costs resulting from the format for production (e.g., requests to produce in hard copy as well as electronic form)					
11	Finding an Expert assistance to assist in discovery and retrieval of evidence					
12	Determining what evidence to collect first i.e. drawing the order of Volatility.					
13	Facilitating On-site inspection of a party's computer system by an opposing party.					
14	Reconstruction of deleted documents without altering the evidence					
15	Handling conflict of interests between provisions/requirements of the Law and collected evidence					
16	Resolving technological incompatibility between storage media & device for restoring the media that could have the evidence.					
17	Preventing permanent destruction of information storage media					
18	Identifying the best format for the evidence production					
19	Access to judicial tools by law enforcement agencies for computer based discovery					
20	Authentication of collected evidence					

14) If you wish to add any additional experiences or ideas from which you think the area of computer forensics and the law might benefit as issues related to ICT legislation initiatives in the country are discussed, please provide them here: -

-----

-----

-----

-----

**Thank you for your participation.**

## Appendix 3: List of the Respondent Banks

Source: Central Bank of Kenya

	Name of the Bank	Address & Contacts of Head Office
1	African Banking Corporation Ltd. ABC Bank, Mezzanine Floor, Koinange Street. Nairobi	Box 46452, Nairobi. Tel. 223922, 251540/1, 226712, 248978 Fax 222437, Telex: 22069 E-mail: mailto:abc@form-net.com
2	Akiba Bank Ltd. Fedha Towers, Muindi Mbingu Street. Nairobi	Box 49584, Nairobi. Tel. 331709, 218360/1, 249633/4, 249670/1/2 Fax 225694, Telex: 22060 E-mail: admin.ho@akibabank.com www.akibabank.com
3	Bank of Baroda Bank of Baroda building, Corner of Tom Mboya and Mandalane street, Nairobi	Box 30033, Nairobi. Tel: 227869, 337911-3 Fax 333089, E-mail: barodabk_ho@kenyaweb.com
4	Bank of India Kenyatta Avenue Nairobi	Box 30246, Nairobi. Tel: 221414-7, 218063, 218871. Fax 229462, Telex: 22715 E-mail: boilo@calva.com
5	Barclays Bank of Kenya Ltd. Barclays plaza, Loita Street.	Box 30120, Nairobi. Tel: 332230, Fax 213915, Telex:22725 E-mail: info@barclays.com; www.barclays.com
6	CFC BANK Ltd. CFC Centre, Chiromo Road, Westlands.	Box 72833, City Square, Nairobi.00200 Tel: 3752900-4, 3741861 Fax 3752905/7 Telex:22814.
7	Chase Bank (Kenya) Ltd. Prudential Assurance Building, 6th floor, Wabera Street.	Box 64042, City square, Nairobi. 00200 Tel. 244035, 245611,252385 Fax 246334, Email: info@chasebank.co.ke
8	Chaterhouse Bank Ltd. Longonot Place,6th floor Kijabe Street.	Box 43252, Nairobi. 224842, 224920, 242246/53 Fax 219058,223060 Telex: 23041 E-mail: info@charterhouse-bank.com
9	Citibank N.A. Citibank House Upper Hill Road	Box 30711,GPO, Nairobi. 00100 Tel: 2711221, 222248 Fax: 2714810, Telex: 22411, 22432
10	Commercial Bank of Africa Ltd. Wabera Street	Box 30437, Nairobi. Tel: 228881, 340200, Fax: 335827, Nairobi. Email: cba@cba.co.ke; www.cba.co.ke
11	Consolidated Bank of Kenya Ltd. Consolidated Bank House	Box 51133, Nairobi. Tel: 340551, 340830, 340920 Fax: 340213.

	Koinange Street	Telex: 22482 E-mail: <a href="mailto:headoffice@consolidated-bank.com">headoffice@consolidated-bank.com</a> <a href="http://www.ipckeny.org/docs/www.consolidated-bank.com">http://www.ipckeny.org/docs/www.consolidated-bank.com</a>
12	Co-operative Bank of Kenya Ltd. New Location-(HQ) Co-operative house Haile Selassie Ave.	Box 48231,GPO, Nairobi. Tel: 225579, 228453/7, 251290/9 Fax: 227747, 246635 Telex: 22938 Email: <a href="mailto:coopbankmd@form-net.com">coopbankmd@form-net.com</a> <a href="http://www.co-opbank.co.ke/">http://www.co-opbank.co.ke/</a>
13	Bank of Africa (Former Credit Agricole Indosuez Re-insurance Plaza Taifa Road	Box 69562, Nairobi. Tel 221175, 210546 Fax: 214166,211477 Telex: 23091 E-mail: <a href="mailto:mailto:user@ke.ca-indosuez.com">mailto:user@ke.ca-indosuez.com</a>
14	Credit Bank Ltd. Ground Floor, Mercantile House Koinange Street	Box 61064, Nairobi Tel 222300, 222317, 220789, 332015 Fax: 216700 Telex: 23050 E-mail: <a href="mailto:cblnbi@creditbankltd.com">cblnbi@creditbankltd.com</a>
15	Development Bank of Kenya Finance House Loita Street	Box 30483, Nairobi. Tel: 340426, 340478, 340416, 3404198 Fax: 338426 E-mail: <a href="mailto:dbk@africaonline.co.ke">dbk@africaonline.co.ke</a>
16	Diamond Trust Bank Kenya Ltd. Nation Centre, 8th floor Kimathi Street	Box 61711,City square, Nairobi 00200 Tel: 210988/83, 210985/86 Fax 336836, Telex: 23177 E-mail: <a href="mailto:user@dtbkenya.co.ke">user@dtbkenya.co.ke</a>
17	Dubai Bank Kenya Ltd. ICEA Building Kenyatta Avenue	Box 11129, Nairobi 00400 Tel: 330562-6 Fax: 245242, Telex: 22596 E-Mail: <a href="mailto:info@dubaibank-kenya.com">info@dubaibank-kenya.com</a>
18	Equatorial Commercial Bank Ltd. Sasini House Loita Street	Box 52467, Nairobi Tel: 331122, 338398, 330611, 221114, 338908 Fax 331606, Telex: 245242 Email: <a href="mailto:ecd@saamnet.com">ecd@saamnet.com</a>
19	Fidelity Commercial Bank 7th Floor, IPS Building Kimathi Street	Box 34886, Nairobi Tel: 242348, 244187 Fax 243389, E-mail: <a href="mailto:customerservice@fidelitybankkenya.com">customerservice@fidelitybankkenya.com</a>
20	Fina Bank Ltd. Fina House Kimathi Street	Box 20613,City Square, Nairobi. 00200 Tel: 240798, 337002, 222580 Fax 337082, E-mail: <a href="mailto:mailto:banking@finabank.com">mailto:banking@finabank.com</a> <a href="http://www.finabank.com">www.finabank.com</a>
21	First American Bank of Kenya First American Bank Centre.	Box 30691, Nairobi Tel: 2710455/6, 2713255, 2719877

	Nyerere Avenue	Fax 333868, Telex: 22398 E-mail: fabk@africaonline.co.ke
22	Guardian Bank Ltd. 6th Floor, View Park Towers Monrovia Street	Box 46983, Nairobi Tel: 333877, 228087, 214460, 214070 Fax 229248, Telex: 23214 E-mail: mailto:gblho@africaonline.co.ke
23	Giro Commercial Bank Ltd. Giro House Kimathi Street	Box 46739, Nairobi. Tel: 330129, 339519, 216005, 330135/7/9 Fax: 336991/210679 Telex: 22013 E-mail: gcbl@swiftkenya.com
24	Housing Finance Rehani House Muindi Mbingu street	Rehani House, Kenyatta Avenue P.O. Box 30088, Nairobi 00100 Tel: 020-317474/221101 Email: rehani.branch@housing.co.ke
25	Habib Bank AG Zurich National House Koinange Street	Box 30584, Nairobi. Tel: 33984-5, Telex: 22982 E-mail: habibbank@form-net.com
26	Habib Bank Ltd. Exchange Building Koinange Street	Box 6906, Nairobi. Tel: 246613, 246641 Telex: 22238 E-mail: hblronbi@africaonline.co.ke
27	Imperial Bank Ltd. Bunyala road Upper Hill	Box 44905, Nairobi. Tel: 2719617/31/52, 342380/73-75, 25284/5 Fax: 2719705/498, 250137 Email: impbank@iconnect.co.ke
28	Industrial Development Bank Ltd. Bima House Harambee Avenue	Box 44036, Nairobi. Tel: 337079 Fax: 334594 Telex: 22339 Email:mailto:%20bizcare@idbkenya.com
30	Investment & Mortgages Bank Ltd. I&M Bank Tower 2nd Ngong Avenue	Box 30238,GPO, Nairobi 00100. Tel: 2711994-8 , 310105-7 Fax: 2713757/2716372 Telex: 22178 E-mail: invest@imbank.co.ke www.imbank.co.ke
31	Kenya Commercial Bank Ltd. Kencom House Moi Avenue	Box 53290, Nairobi. Tel:339441/3, 339450/2, 339446/9 Fax: 338037,336422,216077 Telex: 23085 E-mail: kcbhq@kcb.co.ke www.kcb.co.ke
32	K-REP Bank Ltd. Naivasha Road, Riruta	Box 39312, Nairobi. Tel: 571511, 573169, 573236/45/67, 573141/8 Fax: 573178/711645, E-mail: registry@k-repbank.com

33	Middle East Bank (K) Ltd. Mebank Tower Millimani Road, Kenyatta Avenue	Box 47387, GPO, Nairobi 00100. Tel: 335168-72 Fax: 336182 ; Telex: 23132 E-mail: mailto:mekkenya@nbnet.co.ke
34	National Bank of Kenya Ltd. National Bank of Kenya Building Harambee Avenue	Box 72866, Nairobi. Tel: 226471-8, 339690 Fax: 330784, Telex: 25743 Email: info@nationalbank.co.ke www.nationalbank.co.ke
35	National Industrial Credit Bank Ltd. NIC House Masaba Road	Box 44599, GPO, Nairobi 00100 Tel: 2718200, 2888000, 2718199 Fax: 2888505/13 Email: nic@iconnect.co.ke nic-bank.com/
36	Paramount Universal Bank Ltd. Sound Plaza, Westlands	Box 14001, Nairobi. Tel: 449256 Fax: 449265 E-mail: pbl.bank@africaonline.co.ke
37	Prime Bank Ltd. Kenindia House Loita Street	Box 43825, GPO, Nairobi. 00100 Tel: 4203000, 4203111/01, 4451582-9 Fax: 4451247 Telex: 23224 Email: headoffice@primebank.co.ke
38	Southern Credit Banking Corporation Ltd. Reliance Bank Centre, Westlands	Box 66171, Nairobi. Or Box 11666 Nairobi 00400 Tel: 220939, 220948 Fax: 246309, 221338 Email: admin@ho.southern-credit.com
39	Stanbic Bank (K) Ltd. Stanbic Bank Building Kenyatta Avenue	Box 30550, Nairobi. Tel: 335888, 332805 Fax: 229287, 330227 Telex: 25207; 22397 Email: stanbic@africaonline.co.ke; www.stanbic.co.ke
40	Standard Chartered Bank (K) Ltd. Stanbank House Moi Avenue	Box 30003, GPO, Nairobi 00100 Tel: 330200, 331210, 3209300 Fax: 214086, 223380 Telex: 22209 Email: mdsoffice@ke.standardchartered.com
41	Trans-National Bank Ltd. Trans-National Plaza Mama Ngina Street	Box 34353, Nairobi. Tel: 224234-6, 339201-4, 339225, 339223 Fax: 339227, Telex: 23231 E-mail: tnbl@form.com
42	Victoria Development Bank Ltd. 2nd Floor, Victor Towers, Upper Hill	Box 41114, GPO, Nairobi 00100 Tel: 2719499, 2719815, 2710271 E-mail: Victoria@vicbank.com