

**UNIVERSITY OF NAIROBI
SCHOOL OF COMPUTING AND INFORMATICS**

**DIGITAL FORENSICS FRAMEWORK
FOR KENYAN COURTS OF LAWS**


1

OBWAYA MOGIRE - P56/71598/2008

**SUPERVISOR
CHRISTOPHER A. MOTURI**

APRIL 2011

**Submitted in Partial Fulfillment of the Requirement of the Master
of Science Degree in Information Systems**



Digital Forensics: Digital Forensics Framework for Kenyan Courts of laws

University of NAIROBI Library

0478804 8

DECLARATION

I, **Obwaya Mogire**, confirm that this research project and the work presented in it is my own achievement. To the best of my knowledge, this research work has not been carried out before or previously presented to any other education institution in the world of similar purposes or forum.

r

Sign ifega*.

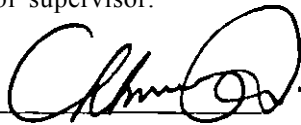
Date a i otf 2-0W

Name: **Obwaya Mogire**

Reg. No: **P56/71598/2008**

This research project has been submitted for examination with my approval as the University of Nairobi supervisor.

Sign



Date

Ap **aLMi <k?H**

Name: **Christopher Moturi**

Deputy Director

School of Computing and Informatics

University of Nairobi

DEDICATION

*To my wife,
Bilia*

*And
My lovely children
Imelda and Feron*

I truly cherish you all.

God bless my family.

ACKNOWLEDGEMENT

First and foremost, I thank my supervisor, **Christopher A. Moturi**. You have been my mentor, a never ending fount of moral support. You have given so much of yourself to help me succeed in this research work. Your perspectives, insights, experiences, and support helped illuminate some of the complex influences and interplays that are shaping the growth and development of digital forensics around the world.

I would also like to thank panel committee for their helpful ideas and comments. The constructive criticisms of **Tonny K. Omwansa** and **Mutahi Theuri** from the School of Computing and informatics, University of Nairobi fuelled me further. Your inputs during the proposal and progress presentations were most invaluable. It is these that offered me platforms upon which I was able to refine this work. In addition, I wish to acknowledge the entire School of Computing and Informatics family for their support and unity of purpose which has made SCI conducive environment for learning.

Gargantuan appreciation goes to my wife **Bilia** and my children **Imelda** and **Feron** for understanding this process. With your encouragement and understanding it gave me hope. My daughter who could not sleep because of glaring colors from my laptop's mouse past midnight and who would occasionally delete my work made me more keen on reviewing my work every now and again; to her much appreciation.

Finally, my utmost gratitude goes to the Almighty God for giving me good health and energy without which I would not have come this far. Thank You Lord.

"The search for truth is in one way hard and in another easy -for it is evident that no one of us can master it fully, nor miss it wholly. Each one of us adds a little to our knowledge of nature, and from all the facts assembled arises a certain grandeur".

God bless you all.

ABSTRACT

We are living in the knowledge age where information and knowledge has become of the most sought after commodity as characterized by proliferation of digital devices and systems. This has seen a paradigm shift in the world where there is an increasing need for Digital Forensics (DF) as a vehicle that organizations can use to provide good and trustworthy evidence and processes. Previous research however points out that developing countries have not yet derived expected benefits from DF technology since very few organizations have the structures in place to enable them to conduct cost effective, low-impact and efficient digital investigations. The adoption, proliferation and maturation of digital forensics in Kenya have been slow due to improper regulatory policies, procedures/processes, technologies, standards, legal and governance challenges.

The purpose of this research was to develop a digital forensics framework that will serve as a blueprint for Kenyan courts of laws in apprehending digital criminals. Existing DF models were surveyed and then adopted to create a specific application framework. Towards achieving this goal, the research investigated best practices, standards, regulatory policies, procedures, technologies, governance, legal systems and people in place and explored some areas in the legal system where digital forensics evidence is most likely to be questioned. To validate the framework, the research methodology employed in this research was a combination of descriptive survey and case study.

The findings of this study have various implications for research as well as practice. For research, best practices, standards, regulatory policies, procedures, technologies, governance and people are critical to influencing digital evidence admissibility in courts. For practice, the findings of this study provide a generic framework for implementation of Digital Forensics. The finding can be used by both government and private agencies in developing countries like Kenya as a guide in providing Digital Forensics services whether Internal investigation, disciplinary hearing or court case.

Keywords: Digital forensics, e-evidence, admissibility, Kenyan courts.

TABLE OF CONTENTS

DECLARATION.....	i
DEDICATION.....	ii
ACKNOWLEDGEMENT.....	iii
ABSTRACT.....	iv
TABLE OF CONTENTS.....	v
List of Abbreviations.....	vii
List of Figures.....	viii
List of Tables.....	ix
CHAPTER ONE:INTRODUCTION.....	1
1.1 Overview.....	1
1.2 Background Information.....	2
1.3 Problem Statement.....	3
1.4 Research Objectives.....	4
1.5 Research Questions.....	4
1.6 Significance of the Research.....	5
1.7 Project Justification.....	5
1.8 Scope of the Study.....	6
1.9 Assumptions and Limitations.....	6
CHAPTER TWO:LITERATURE REVIEW.....	7
2.1 Introduction.....	7
2.2 Basics of Digital Forensics.....	8
2.3 Existing Digital Forensics Frameworks.....	20
CHAPTER THREE:CONCEPTUAL FRAMEWORK.....	29
3.1 Introduction.....	29
3.2 Deriving the Conceptual Framework.....	29
3.3 Elements of the Conceptual Framework.....	31

CHAPTER FOUR: RESEARCH METHODOLOGY	37
4.1 Research Design.....	37
4.2 Target Population and Sampling Frame.....	37
4.3 Research Instruments.....	38
CHAPTER FIVE: FINDINGS, ANALYSIS & INTERPRETATION	41
5.1 Introduction.....	41
5.2 Data Processing and Analysis.....	41
5.3 Detailed Analysis of Responses Questionnaire.....	46
CHAPTER SIX: VALIDATED FRAMEWORK	67
6.1 Introduction.....	68
6.2 Validated Framework.....	68
6.3 Framework Validation.....	71
CHAPTER SEVEN: CONCLUSIONS & RECOMMENDATIONS	73
7.1 Achievements.....	73
7.2 Recommendations.....	75
7.3 Further Research.....	75
7.4 Limitations of the Study.....	76
APPENDIX A: REFERENCES	77
APPENDIX B: QUESTIONNAIRES	81
APPENDIX C: QUESTIONNAIRE ITEMS	87
APPENDIX D: MODIFICATION INDICES	89

List of Abbreviations

ACFE	Association of Certified Fraud Examiners
AMOS	Analysis of Moment Structures
CCK	Communications Commission of Kenya
CFA	Confirmatory Factor Analysis
CIA	Confidentiality Integrity and Availability
COBIT	Control Objectives for Information and related Technology
DF	Digital Forensics
DFRW	Digital Forensics Research Workshop
DFI	Digital Forensics Investigations
DFMM	Digital Forensics Management Model
GFI	Goodness of Fit Index
HTCLA	High Technology Crime Investigation Association
ICI	Information and Communications Technology
IIA	Institution of Internal Auditors
IJCSNS	International Journal of Computer Science and Network Security
ISACA	Information System Audit and Control Association
ISSA	Information System Security Association
ISO	International Organization for Standardization
KACC	Kenya Anti-Corruption Commission
PDA	Personal Digital Assistant
PWC	Price Water Coopers
RRR	Reconnaissance Reliability Relevancy
RM	Reference Model
RMSEA	Root Mean Square Error of Approximation
SIM	Subscriber Identity Module
TCP/IP	Transmission Control Protocol/Internet Protocol
SPSS	Statistical Packages for Social Sciences

List of Figures

Fig.2. 1: Relationship between DF, Computer Forensics, Physical and other Forensics..	11
Fig.2. 2: Digital Forensics Guiding Principles.....	11
Fig.2. 3: I.T Security Fundamentals to Digital Forensics.....	12
Fig.2,4: Indicators of Good DF Practices.....	13
Fig.2. 5: Basic Principles of Admissibility.....	15
Fig.2. 6: Fundamental Principle of DFI.....	16
Fig.2. 7: DFI Extended Model.....	21
Fig.2. 8: Digital Forensics and the Legal System Model.....	22
Fig.2. 9: An Extended Model of Cyber Crime Investigation.....	23
Fig.2. 10: Dimensions of Digital Forensics.....	24
Fig.2. 11: Dimensions of Integrated Digital Forensics in Information Assurance.....	25
Fig.2. 12: Dimensions of Sommer Digital Forensics.....	26
Fig. 3.1: Conceptual Digital Forensics Framework for Kenyan Courts of Laws.....	30
Fig 5. 1: Reliability Analysis of the Kenyan Courts Questionnaires.....	44
Fig 5. 2: Reliability Analysis of the CID Forensics Lab Questionnaire.....	45
Fig 5. 3: KMO and Bartlett's Test.....	46
Fig 5.4: Rating of Experience in DF field.....	48
Fig 5.5: Existence of Modern and Equipped DF Lab.....	49
Fig 5. 6: Technology Determines Reliability of DF services.....	50
Fig 5. 7: Availability of Enough Trained and Qualified staff on DF.....	52
Fig 5. 8: Training key to DF Services.....	53
Fig 5. 9: Regular Training and Awareness of Staff on DF Issues.....	54
Fig 5. 10: DF Legal and Ethical, Policies & Procedures Awareness.....	57
Fig 5. 11: Current Legal Framework Addresses DF.....	58
Fig 5. 12: Proper Legal Framework will Enhances DF.....	59
Fig 5. 13: Adoption, Proliferation and Maturation of DF Depend on Governance.....	61
Fig 5. 14: Scientifically Sound Procedures on DF.....	63
Fig 5. 15: Good Processes Guarantee Admissibility of DF.....	64
Fig. 6. 1: Framework for Digital Forensics for Kenyan Courts of Laws.....	69

List of Tables

Table 2. 1: The Five Phases of DFL.....	19
Table 2. 2: Summary of the Reviewed Models.....	28
Table 3. 1: The Conceptual Framework Dimensions.....	35
Table 5. I: Gender Distribution.....	46
Table 5. 2: Age Distribution.....	47
Table 5. 3: Education Level Distribution.....	47
Table 5. 4: Income Level Distribution.....	48
Table 5. 5: Existence of Modern and Equipped DF Lab.....	50
Table 5. 6: Technology Determines Reliability of DF services.....	50
Table 5. 7: Technology and DF Services Correlation.....	51
Table 5. 8: Availability of Enough Trained and Qualified Staff on DF.....	53
Table 5. 9: Training Key to DF Services.....	54
Table 5. 10: Regular Training and Awareness of Staff on DF Issues.....	55
Table 5. 11: Correlations for Training/Education.....	55
Table 5. 12: Correlations for Training/Education with DF.....	56
Table 5. 13: DF Legal and Ethical, Policies & Procedures Awareness.....	57
Table 5. 14: Current Legal Framework Addresses DF.....	58
Table 5. 15: Proper Legal Framework will Enhances DF.....	59
Table 5. 16: Correlations for Legal and Policies.....	60
Table 5. 17: Correlations for Legal and Policies with DF.....	60
Table 5. 18: Adoption, Proliferation and Maturation of DF Depend on Governance. . . .	61
Table 5. 19: Correlations for Governance.....	62
Table 5. 20: Correlations for Governance with DF.....	62
Table 5. 21: Scientifically Sound Procedures on DF.....	63
Table 5. 22: Good Processes Guarantee Admissibility of DF.....	64
Table 5. 23: Correlation for Processes.....	65
Table 5. 24: Correlation for Processes with DF.....	66
Table 6. 1: Summary of Dimensions of Validated Framework.....	70
Table 6. 2: Chronbach Alpha Test on Validation.....	71
Table 6. 3: Model Summary for Validation.....	72
Table 6.4: Significance and Beta Coefficients for Validation.....	72

CHAPTER ONE

INTRODUCTION

1.1 Overview

Digital Forensics (DF, henceforth) is becoming a business enabler but very few organizations have the structures in place to enable them to conduct cost effective, low-impact and efficient digital investigations (Sommer, 2005). Biros and Weisr (2006) defines digital forensics as "scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters". Digital forensic investigation requires defined procedures that comply with industry practice, organizational practice and appropriate laws, whether as part of a criminal investigation or as part of a more general security incident response. Presenting digital evidence is a unique legal challenge facing digital forensics professionals (Kenneally, 2002). Kenneally notes that evidence in legal cases is admitted or not admitted based on the relative weight of its probative and prejudicial value. In Kenya, digital forensics process is more often than not faced with challenges like admissibility, authenticity, accuracy, relevancy, non-repudiation, reliability, credible, completeness and convincing to juries due to poor standards like ISO 17799 and COBIT, regulatory policies, best practices, procedures/processes, governance, technologies, staff, legal and ethical. The research problem of this project was designed to investigate the current technologies in place, legal framework, regulatory policies and practices and came up with a framework suitable for Kenyan courts of laws.

Chapter 1 introduces the problem area and gives the aim and objective of the study as well as the justification. Chapter 2 reviews the related literature and also looks at available DF models in the world. Based on weaknesses and gaps identified, Chapter 3 gives a conceptual framework. Chapter 4 details the research methodology used while Chapter 5 is discussion and analysis of the findings. Chapter 6 discusses validated framework and lastly Chapter 7 gives conclusions and recommendations.

1.2 Background Information

Biros and Weiser (2006) defines digital forensics as "scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters". Some authors make a clear distinction between computer forensics and digital forensics. Yet, for the purposes of this research, no real distinction is made. Van Solms and Lourens (2006) defines computer forensics as "analytical and investigative techniques used for the preservation, identification, extraction, documentation, analysis and interpretation of computer media (digital data) which is stored or encoded for evidentiary and/or root cause analysis"

All organizations, in particular law enforcement agencies, should have standards, policies and procedures in place that can assist in DF processes. Standards that are important here are ISO 17799 and COBIT. These standards do not cover a forensic investigation, but could be used to aid it. As well as internal standards and policies, there are several legislative measures that support organizations attempting to prosecute digital crimes. In Kenya, there are a number of important Acts that can be referenced. These include the Evidence Act Cap (80) Section 64 and 83 of 2007, Penal Code Act 2007, Criminal Procedures Act 2007 And Communication Bill Act 2007. These, however, do not provide any clear guidelines as to how a forensic investigation should be conducted to ensure legal appropriateness but lay emphasis on prosecution of digital perpetrators. Consequently, an important way for most organizations to protect themselves against digital crime is to institute internal policies and procedures which specify exactly what constitutes harmful action against or within an organization.

Thus far it has been determined that implementing certain standards, like ISO 17799, can be a useful initial step by an organization towards effectively protecting its information and assets. Moreover, that specific regulatory policies, techniques and procedures should also be implemented within an organization to help protect the internal integrity of information and assets. The pertinent legal issues like technologies, training/education, governance, research, policies, processes, people that contributes to the admissibility, authenticity, accuracy, completeness, and convincing to juries of digital evidence that result from a digital forensic is an emerging and interesting area of research.

In our research we set out to review digital forensics and related research in order to get information on how these issues have been addressed. The outcome of our research findings is a validated framework that will serve as a blue print for Kenyan courts of laws. The framework is an adaptation or combination of several existing forensics models.

1.3 Problem Statement

In the current world where information and knowledge has become the most sought after commodity; criminals, competitors and even employees exploit loopholes in current security architectures and control structures to obtain the required information to commit digital crimes. Organizations spend a lot of time, money, and effort in planning for incidents, natural disasters or security breaches by drafting incident response, disaster recovery and business continuity plans. These plans identify an incident and prescribe the best way to recover and continue with the business as quickly as possible. However, according to Sommer (2005), very little thought is given to the identification and preservation of digital evidence and the correct structuring of processes for possible prosecution. Sommer continues to point out that very few organizations have the structures (management and infrastructure) in place to enable them to conduct cost effective, low-impact and efficient digital investigations. Often, when asked for specific digital evidence, most organizations do not have all the evidence available (Clark, 2006).

In Kenya for example according to CCK (2008), a widespread crimes being perpetuated by using mobile phones like terrorism, drug trafficking, money laundering, extortion, fraud, hate messages, and incitement are on increase. But more often than not evidence presented before Kenyan courts of laws are inadmissible due to lack of proper DF framework. This necessitated CCK to institute some regulatory policies like requiring all mobile subscribers to register their SIM card with effect from 2010. (<http://www.cck.go.ke>). However this move still has a number of loopholes which are yet to be addressed. For example enforcing the policies is a challenge both to the service provider and the government due to lack of proper relevant laws.

It is against this background that in this research project, we set out to explore issues of technology, training/education, processes, governance, legal and ethics in Kenyan with a view of understanding DF models used in addressing the issues of digital crimes.

It is from existing gaps that we developed a framework that will provide guidance in digital forensics processes, particularly in developing countries like Kenya.

1.4 Research Objectives

The primary objective of the study was to develop a Digital Forensics Framework that will enhance growth in Digital Forensics by producing forensically sound e-evidence before Kenyan Courts of laws for legal proceedings.

The study was also expected to achieve the following secondary objectives;

1. Investigate the state of existing technologies, regulatory policies and legal frameworks regarding Digital Forensics in key government and private agencies involved in DF in Kenya.
2. Investigate to what extent does technology, processes, regulation, staff, education and governance contributes towards reliability, admissibility and authenticity of Digital Forensics.
3. Test validity of the proposed framework

1.5 Research Questions

The research attempted to answer the following questions as we tried to come up with a digital forensics framework:-

1. Do the existing technologies, policies, process, staff, training/education and legal frameworks if any sufficiently address the issues of Digital Forensics?
2. What are the challenges facing the reliability, admissibility and authenticity of Digital Forensics services?
3. Do the existing legal frameworks sufficiently address the issues of Digital Forensics?

Based on these questions, this research therefore explored digital forensics as a new technology used to provide digital evidence in Kenyan courtroom for successful prosecution.

1.6 Significance of the Research

1. Can be used as a blueprint for further research on Digital Forensics.
2. It can be used to determine whether the current Digital Forensics technologies and legal frameworks adequately address the issues of e-evidence.
3. To create awareness to various key law enforcement agencies both government and private why proper Digital Forensics is important.

1.7 Project Justification

Technological progress in computing, information and communication in the last few years has seen a sporadic increase in numbers of people using the technology. According to Doran (2008), mobile phone proliferation is on the increase with the worldwide cellular subscriber base reaching 4 billion by the end of 2008. Kenya alone, the number of mobile subscribers stands at 20.9 million (CCK, 2010). According to Internet World Stats (2009) and CCK (2009), there were more than 1.8 billion Internet users worldwide and about 4 million Internet users in Kenya by the end 2009 (<http://www.cck.go.ke>). As a result, digital systems is driving digital economy translating to convenience, efficiency and reduced operational cost due to these digital devices.

However on the other hand there is an increase in digital crimes like fraud, hacking, cyber stalking, embezzlement, forgery, harassment, discrimination, sabotage, copyright infringement, security violations, illegal spreading of pornographic materials, theft, virus attacks among others. According to CCK (<http://www.cck.go.ke>), the increase of such criminal activity places a strain on law enforcement and governments. This concern has seen CCK put up regulatory measures in place by requiring all mobile subscribers in Kenya register their SIM cards.

Courts no longer require only document-based evidence but also electronic-based evidence. However according to Ayers and Jansen (2007), Law enforcement and digital forensics still lag behind when it comes to dealing with digital evidence obtained from digital devices. The demand for digital based evidence by courts means the need for proper Digital Forensics is becoming more crucial. An assessment of existing DF technologies and regulatory framework in CID, KACC and PWC was to help to determine the current situation in order to develop a Digital Forensics framework and recommend specific changes arising from the research findings.

It is against this backdrop that it was absolutely necessary to provide a framework that will act as a blueprint in the field of DF. In this research, our main objective was to develop a sound DF framework for digital forensics for the Kenyan courts of laws. The proposed framework is tailored to the needs of Kenya as a developing country characterized by lack of proper technologies and regulatory framework.

1.8 Scope of the Study

Digital forensics offers many benefits and opportunities for Kenyan courts of laws including reliability, efficiency, timeliness, accuracy among others thus promoting admissibility and improving performance/delivery and methodologies. By allowing effective and increased adoption of digital forensics by Kenyan courts of laws, it will offer them an opportunity to overcome the problem of increased inadmissibility of digital evidence presented before the court. As such, the study undertook an assessment of digital forensics state in Kenya. The various dimensions in DF required to produce forensically sound evidence were the centre of this study. The study was however restricted to CID, KACC, HIGH COURT and PWC in accessing current enabling technology, governance, regulatory policies, best practices, and standards, processes, legal and training/education on DF.

1.9 Assumptions and Limitations

1. The study required good level of cooperation from all various key players in the field. An assumption at this point was made that the key players will indeed cooperate in giving information.
2. The various key agencies to be interviewed have documented resources relating DF technologies, processes, practices, legal frameworks and regulatory policies.
3. There is flow of information between various concern DF players.

The main limiting factors was that the key players involved consider themselves and their activities confidential and as such, getting the information involved a lot of protocols which meant the research took a lot of time and resources.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Technological progress in computing, information and communication in the last few years has seen a sporadic increase in numbers of people using the technology. As a result, digital systems are driving digital economy translating to convenience, efficiency and reduced operational cost. However as the popularity of these digital systems grows, there is great concern of the security of the information systems. Criminals, competitors and even disgruntled employees exploit any loopholes in current security architectures and control structures, use anti-forensic techniques and tools to hide their traces and apply forensic tools and techniques to obtain the required information to commit digital crimes like terrorism, drug trafficking, money laundering, extortion, fraud, hate messages, and incitement, hacking, cyber stalking, embezzlement, forgery, harassment, discrimination, sabotage, copyright infringement, security violations, illegal spreading of pornographic materials, theft, virus attacks among others. The increase of such criminal activity places a strain on governments' law enforcement and private agencies. As a result, these agencies spend a lot of time, money, and effort in planning for incidents, natural disasters or security breaches by drafting incident response, disaster recovery and business continuity plans. These plans are meant to identify an incident and prescribe the best way to recover and continue with the business as quickly as possible. However, very little thought is given to the identification and preservation of digital evidence and the correct structuring of processes for possible prosecution of digital criminals (Sommer, 2008). Towards this end, Digital Forensics is becoming a vehicle that organizations use to provide good and trustworthy evidence and processes. Digital Forensics is defined as scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters (Biros and Weiser, 2006).

According to Biros and Wisser, the primary goals of digital forensic analysis are fivefold:

- i) to identify all the unwanted events that have taken place,
- ii) to ascertain their effect on the system,
- iii) to acquire the necessary evidence to support a lawsuit,
- iv) to prevent future incidents by detecting the malicious techniques used and
- v) to recognize the incitement reasons and intendance of the attacker for future predictions.

However, previous research has found that developing countries have not derived the expected benefits from Digital Forensics (Clark, 2006). Consequently, there is still doubt about how DFs will be a business enabler in developing countries as we embrace digital economy (Sommer et al., 2007). Thus, understanding digital forensics processes and practices has become an important issue. This is likely to resolve the problem of digital crime resulting from the proliferation of digital technology systems in developing countries like Kenya.

2.2 Basics of Digital Forensics

The merging of computer systems and telecommunications industry has had profound influence in the modern society (Theodore 2005). The telecommunications industry provided network infrastructure through which we can connect computers, Personal Digital Assistant (PDAs, henceforth) and mobile phones to communicate and share information. This integration therefore necessitates a multidisciplinary approach to network and system management in order to safeguard information confidentiality and integrity while making it readily available to only authorized users.

According to Mani (2006), the traditional telecommunication system has been known to be reliable and dependable. Mani points out that this is partly because of the efficient management of the telephone network using proven network management tools, protocols and security mechanisms. On the other hand, wireless network technologies are still at an evolution mode.

This means that the wireless network management tools, protocols and security mechanisms used does not guarantee the same reliability as that of wired networks. The impact of such technology on the world provides limitless benefits to individuals, business, commerce and industry. Unfortunately, as the technology develops so does the vulnerability of systems to failure, to unauthorized access and to attack. Digital crime has become unfortunate artifact of today's wired and global society. It is no surprise that individuals involved in deviant and or criminal behavior have embraced technology as a method for improving or extending their criminal tradecraft. As a result, our notions of evidence and what constitutes potential sources of evidence is drastically changing. Gone are the days when evidence was primarily document based. Today and going forward, evidence is becoming more electronic or digital based and as such the need for the timely identification, analysis and interpretation of digital evidence is becoming more crucial.

Successful prosecution of digital based crime is reliant upon the investigator being able to prove beyond no reasonable doubt who, what, how and when a criminal event occurred within the stringent principles of forensic examination of evidence. In many investigations critical information is required while at the scene or within a short period of time - measured in hours as opposed to days. The traditional forensics approach of seizing a system(s)/media, transporting it to the lab, making a forensic image(s), and then searching the entire system for potential evidence, is no longer appropriate in some circumstances. In cases such as child abductions as rampart in Kenya, pedophiles, missing or exploited persons, time is of the essence; in some cases it is the difference between life and death for the victim(s). With no clear framework, digital crime is of such a nature that it is often difficult for the general public to perceive or to understand that a crime has actually occurred.

Presenting digital evidence before a court of law is a unique legal challenge facing digital forensic professionals (Kenneally, 2002). Kenneally points out that evidence in legal cases is admitted or not admitted based on the relative weight of its probative and prejudicial value. Given that the legal system is based on precedents, forensic investigators must introduce cohesion and consistency in the expanding field of extracting and examining evidence.

Having looked at the impact of ICT technologies, we studied Digital Forensics and its enabling environment, being a business enabler that is driving the digital economy, in Kenya to further research work on how DF can be used to curb the negative impact presented by these ICT technologies and related applications. If Kenya as a country is to reap benefits from these ICT technologies, there is need to understand how Digital Forensics can be applied taking into considerations our existing technologies, legal, training/education, regulatory policies, processes and infrastructure perspectives.

2.2.1 What is Digital Forensics?

Digital Forensics can be defined as the efficient use of analytical and investigative techniques for the preservation, identification, extraction, documentation, analysis and interpretation of computer media which is digitally stored or encoded for evidentiary and/ or root cause analysis and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations (DFRW, 2001 & Reith, 2002). The goal of any forensic investigation is to prosecute the criminals/offenders or determine the root cause of an event and determine who was responsible. DF is more comprehensive than computer forensics. With the emergence of new technologies e.g. wireless communications and the internet, computer forensics has become a subset of DF. Various overlaps with other forensic disciplines exist. Fig. 2.1 is a diagrammatic representation of how digital forensics, computer forensics, physical and other forensic investigations can overlap. The DF investigation must include all aspects, physical evidence for example physical credit cards, printouts, cameras etc. as well as digital evidence. Results from pathological, ballistic and other investigations must be included in an investigation. According to Reith (2002) DF readiness is key factor in all organization, which is the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation.

Digital Forensic investigation

Computer Forensic Investigations

Physical Forensic investigations

Ballistics

Chemical
forensic
investigations

Pathological
forensic
investigation

Fig.2.1: Relationship between DF, Computer Forensics, Physical and other Forensic Investigations; (Reith, 2002)

According to IJCSNS VOL.9 No.8 (2009) digital forensics is modeled around three guiding principles, namely;

- The Complaint,
- The Investigation and
- > The Prosecution.

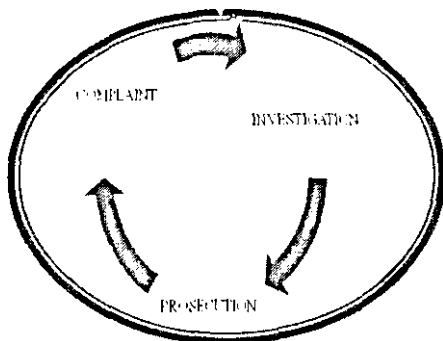


Fig.2. 2: Digital Forensics Guiding Principles; IJCSNS VOL.9 \o.8 (2009)

2.2.2 Security Fundamentals to Digital Forensics

According to Saks & Koehler (2005), we are in a paradigm shift in the evaluation of evidence in the forensic comparison sciences. This is a shift requiring that the evaluation of forensic evidence actually be scientific, including that the reliability of methodologies be testable, and requiring that forensic evidence be evaluated and presented to the courts in a logically correct manner. Losavio and Adams' (2006), notes that the core IT Security fundamentals to digital forensics are; Confidentiality, Integrity and Availability (CIA), as illustrated in (Fig.2.3).

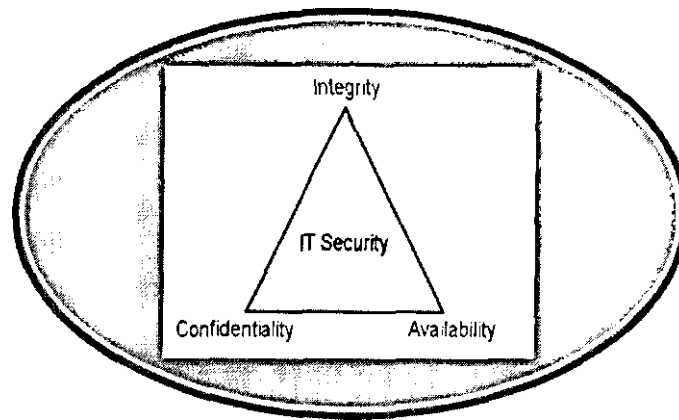


Fig.2.3:1.T Security Fundamentals to Digital Forensics (Losavio and Adams' 2006)

2.2.3 Indicators of Good DF Practices

Good practice must be adhered to in the evidence gathering process otherwise a case or prosecution would be easily jeopardized by shoddy handling. Evidence must comply with the rules for the same. One must account for any changes and the original evidence must be handled as little as possible. Evidence must be of high enough standard to withstand the test of a court process. The admissibility, authenticity, reliability, credibility, curacy and completeness of digital evidence- will heavily rely on how well these axes are developed and managed. Fig.2.4 gives a summary of expected outcome when the above components are well managed.

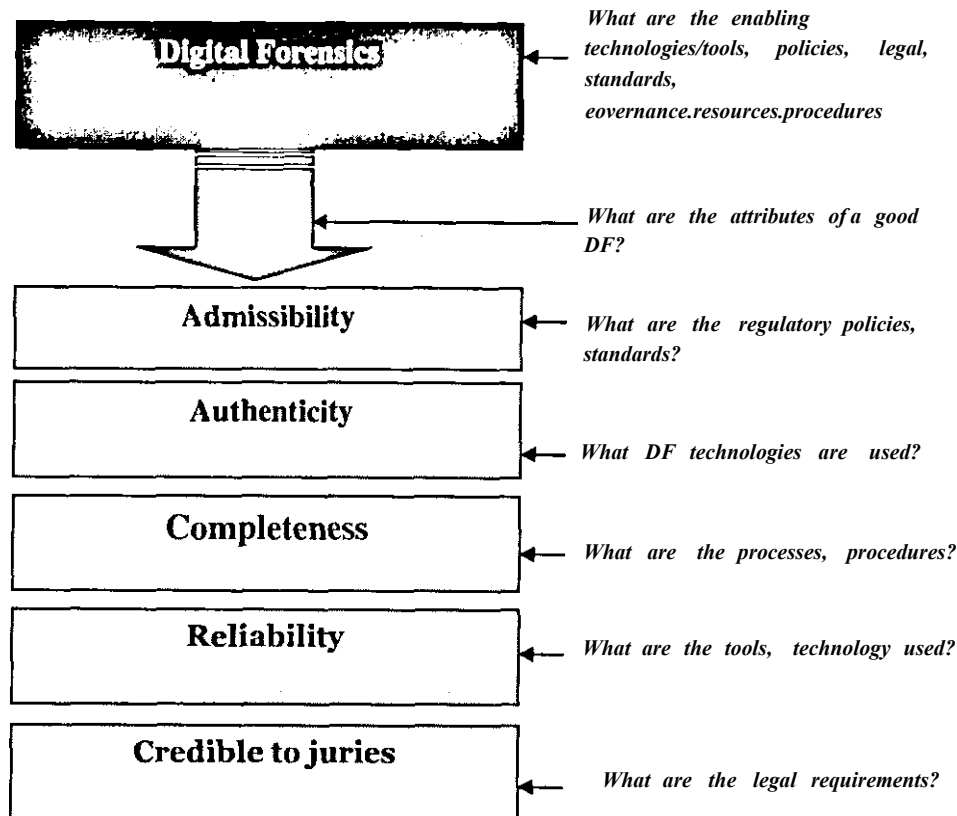


Fig.2. 4: Indicators of Good DF Practices

According to Gordon (2006), good digital forensics practices include;

- # **Principle 1:** No action should be taken by a law enforcement agency or investigator to change data held on a computer, device or storage medium which may be relied upon in court.
- **Principle 2:** In rare circumstances where original data must be accessed, that person accessing it must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3:** An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to scrutinize these processes and arrive at the same result.

• **Principle 4:** The person in charge of the investigation, the case officer, has overall responsibility for ensuring that the law and these principles are adhered to.

However, previous research work on this area is scanty and provides only fragmented insights. If proper legal frameworks suitable for our Kenyan environment are developed, some of the challenges facing DF would be resolved. As a result, the developed Digital Forensics framework for Kenyan courts of laws seeks to introduce cohesion and consistency to the wide field of extracting and examining evidence obtained from a digital device.

2.2.4 Admissibility of e-evidence

"Legal rules which determine whether potential evidence can be considered by a court" (Sommer 2002,) is the definition that will be adopted to define the idea of "admissibility" of the electronic evidence in this research. The issue of whether or not evidence resulting from digital forensic investigation will hold water in court and be accepted as evidence in a case is two-fold. The judges must determine if the evidence was legally obtained and secondly that the integrity of the original data was maintained (McMillian, 2000; Schwartz, 2004; Sommer, 2002). The first issue is if the investigator had a legal right to seize and investigate the suspects' digital device. This requires the investigator to obtain appropriate approval and any necessary documentation such as a search warrant prior to conducting any investigation.

The second aspect of whether or not evidence will hold up in court is in the evidence gathering techniques. The correct investigation software is crucial if any law enforcement/organization ever want to use evidence in court (Schwartz 2004). Schwartz points out that many of the current systems are rarely designed to collect and protect the integrity of the type of data required for legal proceedings in such a way as to remain admissible in court. Investigation software/technology should help security investigators for example to examine local or remote disks, using everything from keyword searches to restoring deleted files, without altering data or metadata (Schwartz, 2004).

The Daubert process, (summarized in Fig2.5), identifies four general categories that are used as guidelines when assessing a procedure suitable for DF in order for the evidence to be admissible;

- **Testing:** Can and has the procedure been tested?
- **Error Rate:** Is there a known error rate of the procedure?
- **Publication:** Has the procedure been published and subject to peer review?
- **Acceptance:** Is the procedure generally accepted in the relevant scientific community?

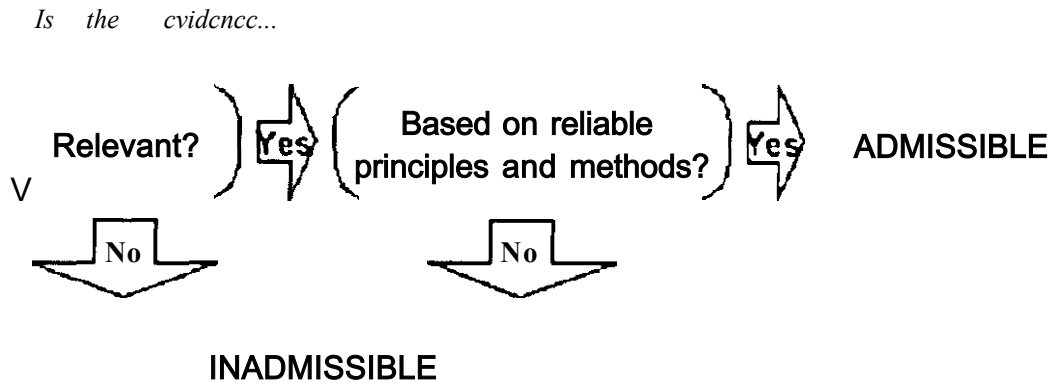


Fig.2.5: Basic Principles of Admissibility

2.2.5 Digital Forensics Investigation (DFI)

Digital Forensics Investigation (DFI, henceforth) is a process to determine and relate extracted information and e-evidence to establish factual information for judicial review. It requires defined procedures that comply with industry practice, organizational practice and appropriate laws, whether as part of a criminal investigation or as part of a more general security incident response. According to Biros and Waiser (2006), to accomplish this requirement, its fundamental principle includes Reconnaissance, Reliability, and Relevancy (R). Fig. 2.6 gives the illustration.

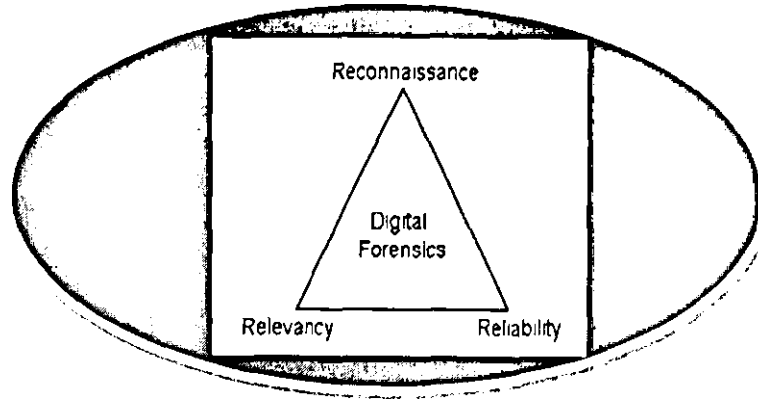


Fig.2. 6: Fundamental Principle of DFI; Biros and Waiser (2006)

Reconnaissance- a digital forensics investigator needs to exhaust different methods, practices and tools that were developed for particular operating environment to collect, recover, decode, discover, extract, analyze and convert data that kept on different storage media to readable evidence. No matter where data are stored, digital forensics investigators should be revealing, and focusing retrieval often the truth behind the data.

Reliability- Chain of evidence should be preserved during extracting, analyzing, storing and transporting of data. In general, chain of evidence, time, integrity of the evidence and the person relationship with the evidence could be collectively considered as the non-repudiation feature of digital forensics. If the evidence cannot be repudiated and rebutted, then the digital evidence would be reliable and admissible for judicial review.

Relevancy- Even though, evidence could be admissible, relevancy of the evidence with the case affects the weight and usefulness of the evidence. If the legal practitioner can advise on what should be collected during the process, time and cost spent in investigation could be controlled better. Table 2.1 gives a summary of DFI stages to be followed to produce forensically sound evidence

Phase

Activities / Processes

Output

<ul style="list-style-type: none">• Monitoring authorization and management support, and obtain authorization to do the investigation• Ensuring the operations and infrastructure are able to support an investigation• Provide a mechanism for the incident to be detected and confirmed• Create an awareness so that the investigation is needed (identify the need for an investigation)• Plan on how to get the information needed from both inside and outside the investigating organization• Identify the strategy, policies and previous investigations• Informing the subject of an investigation or other concerned parties that the investigation is taking place• Determine what a particular piece of digital evidence is, and Identifying possible sources of data• Determine where the evidence is physically located• Translated the media into data• Ensuring integrity and authenticity of the digital evidence e.g. write protection, hashes etc.• Package, transport and store the digital evidence• Preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius• Record the physical scene• Duplicate digital evidence using standardized and accepted procedures• Ensuring the validity and integrity of evidence for later use_	<p>Plan, Authorization, Warrant, Notification, Confirmation</p> <p>Crime type, Potential Evidence Sources, Media, Devices, Event</p>
--	--

- Determine how the data produced, when and by whom
- Determine and validate the techniques to find and interpret significant data
- Extracting hidden data, Discovering the hidden data, and Matching the pattern
- Recognize obvious pieces of digital evidence and assess the skill level of suspect
- Transform the data into a more manageable size and form for analysis
- Recognize obvious pieces of digital evidence and assess the skill level of suspect
- Confirming or refuting allegations of suspicious activity
- Identifying and locating potential evidence, possibly within unconventional locations
- Construct detailed documentation for analysis and Draw conclusions based on evidence found
- Determine significant based on evidence found
- Test and reject theories based on the digital evidence
- Organizing the analysis results from the collected physical and digital evidence
- Eliminate duplication of analysis
- Build a timeline
- Construct a hypothesis of what occurred, and Compare the extracted data with the target
- Document the findings and all steps taken

| ix)g Files, Hie,
i
i Events log,
Data,
Information

2.3 Existing Digital Forensics Frameworks

The Oxford Dictionary defines a framework as "a supporting or underlying structure". A digital forensic framework can be defined as a structure to support a successful forensic investigation. This implies that the conclusion reached by one digital forensic expert should be the same as any other person who has conducted the same investigation. A framework is also dependent on a number of structures. In the case of digital forensics, or forensics in general, legislation has to be considered to be of prominent importance. A forensic investigation has to be conducted in a scientific manner and must comply with all legal requirements. Evidence will have to be collected in this manner irrespective of the purpose i.e. internal investigation, disciplinary hearing or court case. The number of forensic models that have been proposed reveals the complexity of the DF process. Most focus on either the investigation itself or emphasize a particular stage of the investigation. These models have been developed to assist law enforcement in dealing with the shift from document based to digital based evidence (Becbe & Clark, 2004). Every digital forensic model has its own negative and positive attributes. From literature reviewed however, we can have two categories of referenced models in DF;

1. Digital Forensics Investigation (DFI) referenced models
2. Digital Forensics (DF) reference models

2.3.1 Digital Forensics Investigative Reference Models

A reference model (RM) is a universal generic model that can be used as a blueprint in the development of a field (Becker et. al. 2003). It 'provides a conceptual framework that should facilitate the creation of domain-specific application models, or descriptions of specific DFI application domains. Though there are several proposed models, we wish to focus on three RMs that are from DFI processes domain.

2.3.1.1 IJCSNS; Seamus Extended DFI Model

Seamus model is the most latest and covered quite number of process. The model includes the following activities such as planning, identification, reconnaissance, analysis, result, proof and defense, and archive storages. Planning stage includes authorization by obtaining search warrant. Reconnaissance involves gathering evidence, transport and storage. Fig 2.7 represents the said model.

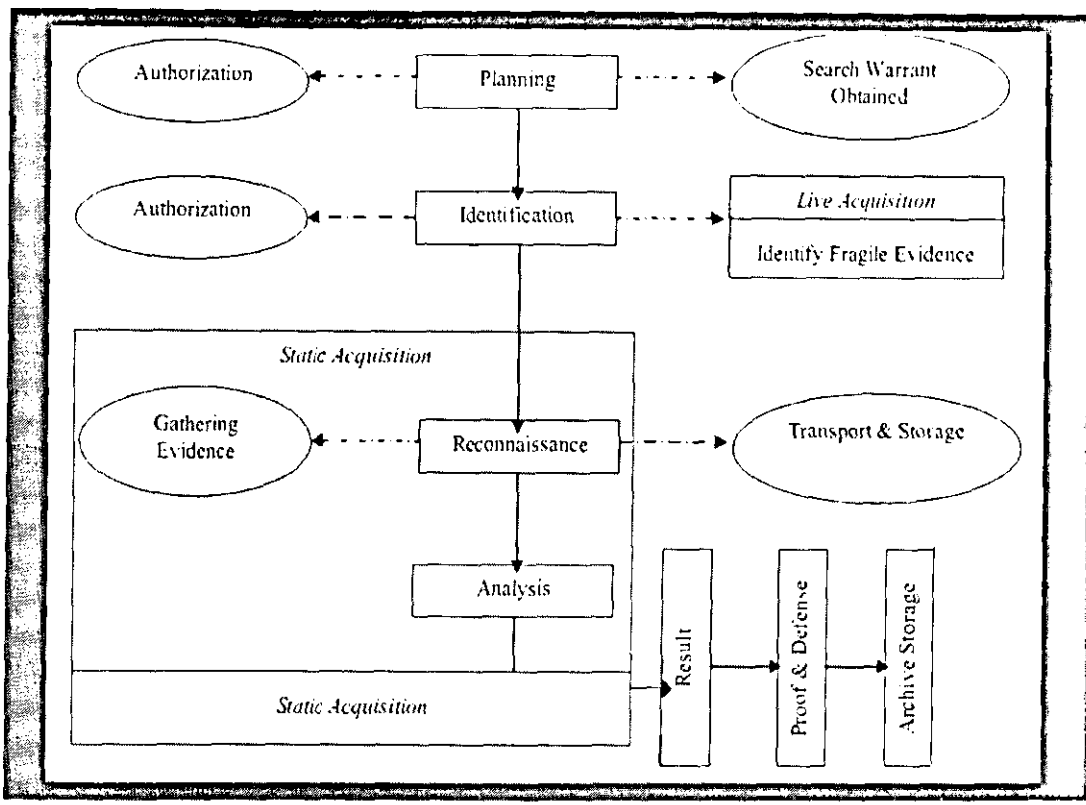


Fig.2. 7: DFI Extended Model (IJCSNS Vol. 9 No.8,2009)

2J.1.2 Digital Forensics and the Legal System Model

The model include the following activities such identification/preparation, search and seizure of evidence, preservation of evidence, examination, analysis and reporting. Documentation takes place in the entire activities. The model captures these stages as legal requirements for a sound DF processes. Fig 2.8 illustrates the model.

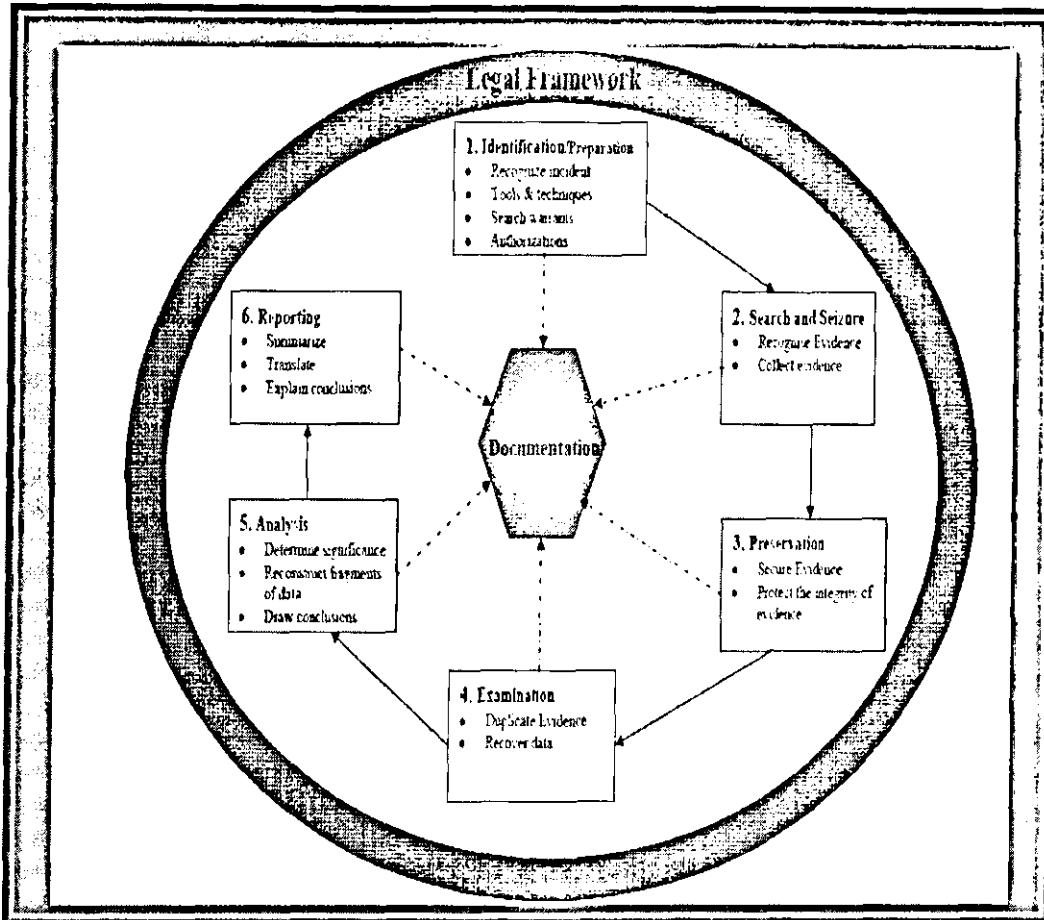


Fig.2.8: Digital Forensics and the Legal System Model; (James Tetteh, Cowan University) Undated

2.3.13 A Hierarchical, Objectives-based I)FI Model

The model include the following activities such as awareness, authorization, planning, notification, search for and identify evidence, collections of evidence, transport of evidence, storage of evidence, examinations of evidence, hypothesis, presentation of hypothesis, proof/defense of hypothesis, and dissemination of information . This model borrows number of activities from IJCSNS model but it adds more dimensions which arc very key to DF processes like digital forensics awareness, regulatory policies, legal frameworks, external control. Fig 2.9 describes the model in detail.

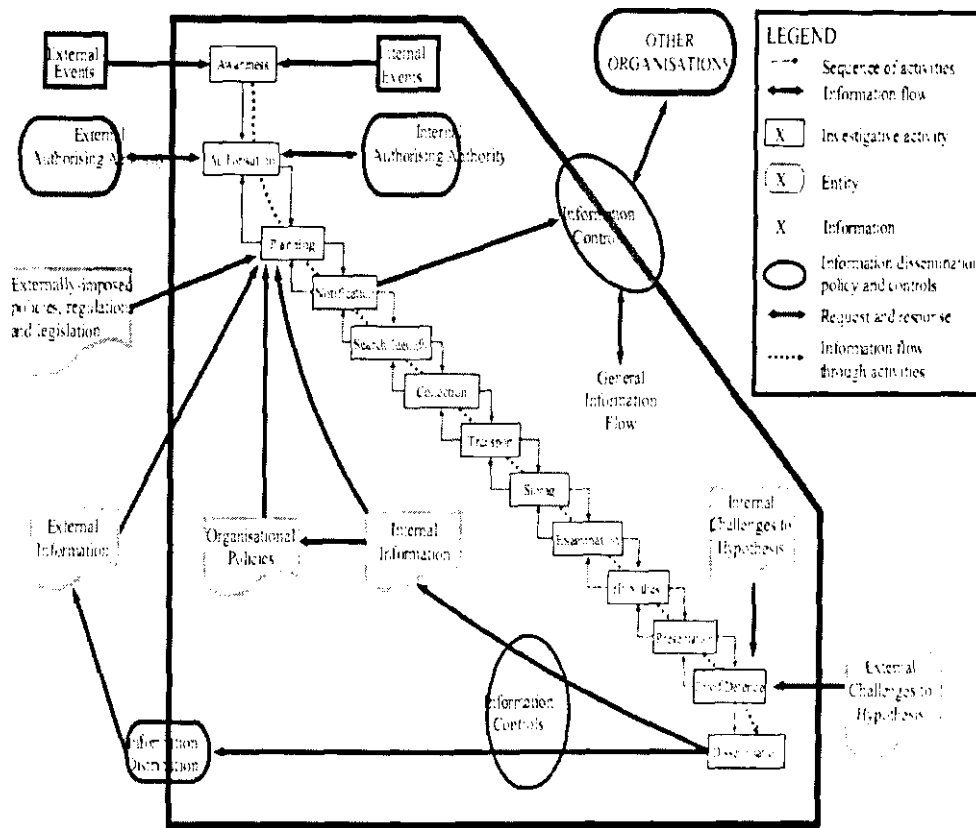


Fig.2. 9: An Extended Model of Cyber Crime Investigation; (Ciardhuain, S. O. 2004); www.ijde.org

2.3.2 Digital Forensics (DF) Referenced Models

Though there are several proposed DF models, we wish to focus on three DF RMs that arc from a technological, people, processes, regulatory policies, training/education and research

2.3.2.1 DF Legal Requirements Framework

This framework captures a very important aspect of DF especially in developing countries. Even though the framework best fits deveopled countries where technology is advanced, we will extract ideas from this model to formulate a new one, that we think will best serve Kenyan legal requiremsnts environment.

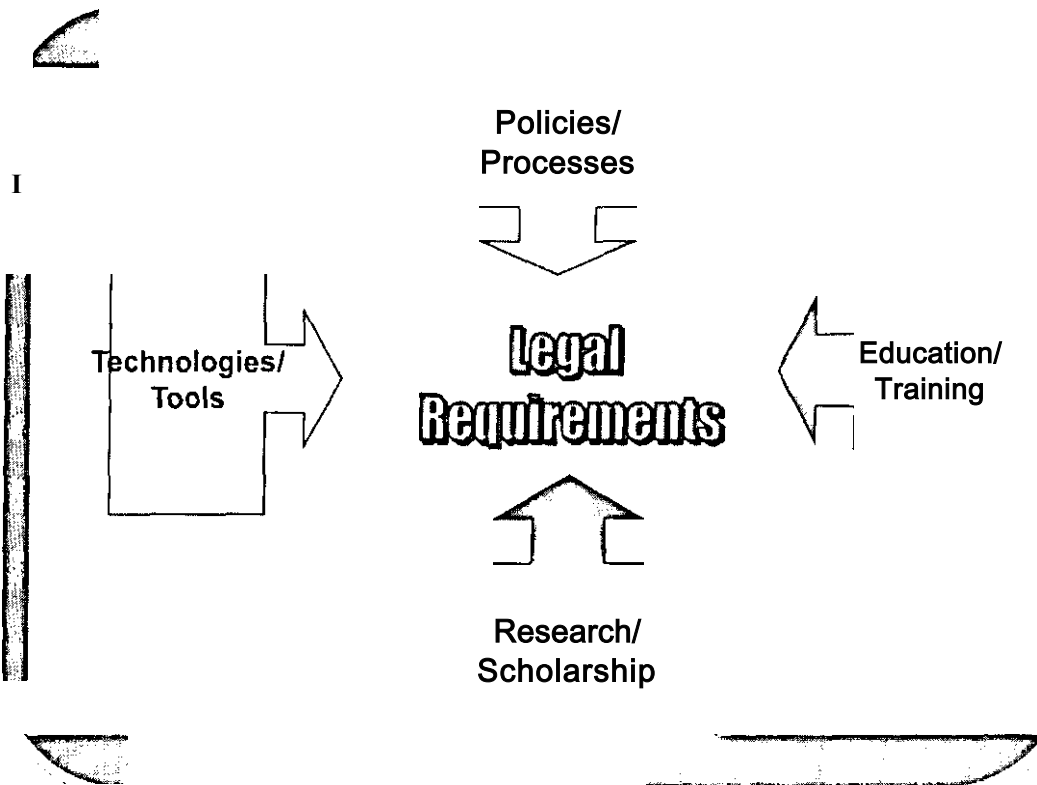


Fig.2.10: Dimensions of Digital Forensics (USA, undated)

2.3.2.2 Integrated Digital Forensics Framework in Information Assurance

Digital forensics should be integrated into the discipline of information assurance as one of its methods. According to McCumber (2005), the security countermeasures are the technologies, policies, practices and human factors (training, vetting employees, etc.) that implement information assurance. These countermeasures are deployed through the three basic information states-transmission, storage and processing; providing three services to system:-Confidentiality, Integrity and Availability. He argues that digital forensics has a function within each cell of the cube (Fig. 2.11), giving it a role in enterprise information systems operations. Thus defining what it means for a country to be "forensically ready" incorporates the full spectrum of information assurance (IA) *e]mcnts:-security, policies, procedures, practices, mechanisms, and security awareness training programs.*

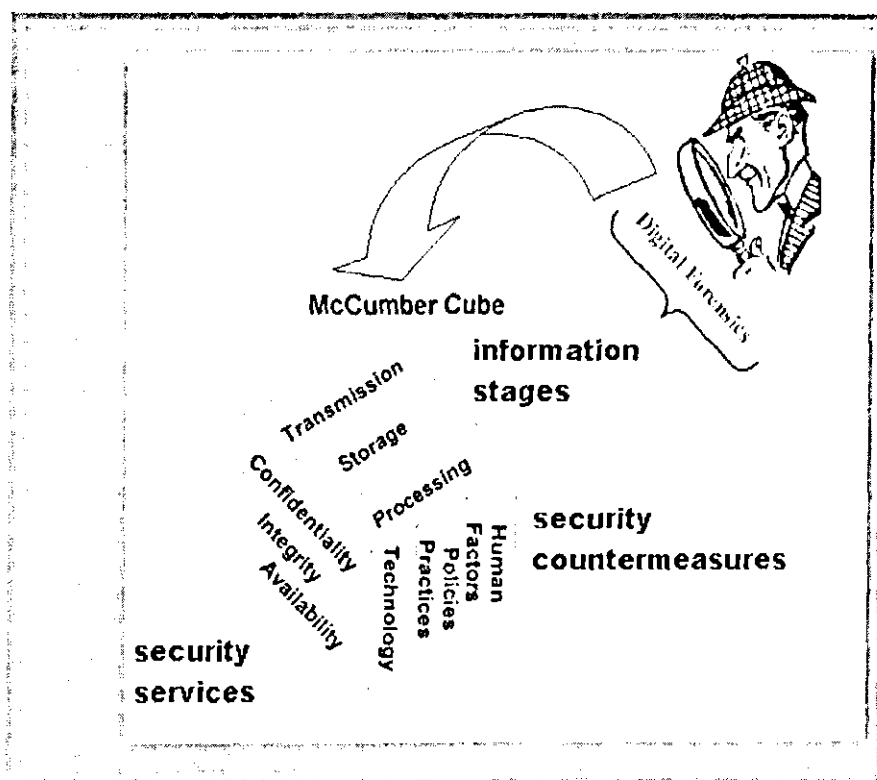


Fig.2. 11: Dimensions of Integrated Digital Forensics in Information Assurance (McCumber, 2005)

Once these basics are in place, the next step is to apply a sound digital forensic framework, which will consistently gather digital evidence suitable for presentation in a court of law. Without sound digital forensics procedures and techniques, many cases of digital crime are left unsolved. The law enforcement agencies investigating the suspicious behaviour often lack the tools, skills, techniques and the financial resources to conduct such an investigation adequately and ensure that the evidence is undisputable in all circumstances. Moreover, there are instances when all of the above have been adequately put in place by an organization, but, due to a lack of proper technologies, regulatory policies, standards, and correct procedure, the evidence collected can easily be disputed as common in developing countries like Kenya.

2.3.2.3 Sommer Digital Forensics Framework

Sommer (2008), suggested that Digital Forensics framework has three dimensions as shown below; *People, Technology and Processes*. This framework captures a very important aspect of DF especially in developing countries. However, the framework subject is only three dimensions that are necessary but not sufficient to a sound DF implementation and management. We therefore find it does not represent the full picture of Digital Forensics.

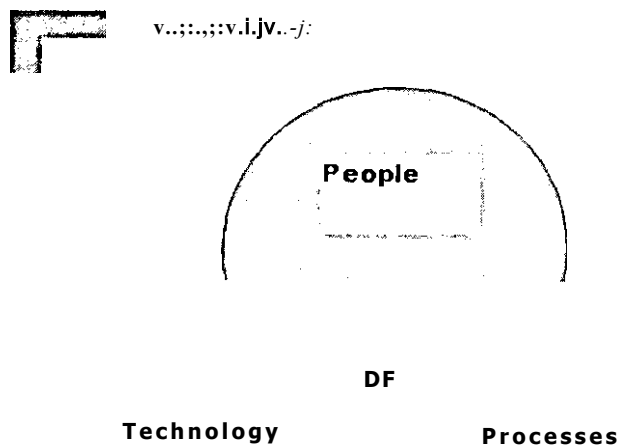


Fig.2.12: Dimensions of Sommer Digital Forensics; (Sommer, 2008)

All the models reviewed have been developed and proposed in environments that are very different from those in developing countries like Kenya. Their emphasis is on technology and regulatory policies dimensions as the backbone of other dimensions of DF. That is possible in developed world since they have access to state of the earth technology and human resources. In developing countries like Kenya however, we face a serious challenge in access and use of technology. As a result we have some additional challenges that must be handled differently. It is our considered view that applying these models in our context may not give expected results. We therefore wish to use them as the basis for further study to come up with DF framework fitting Kenyan legal systems environment. We however wish to adopt USA as the preferred RM in this research. The selection is based on the wide usage of the framework in USA, which gives an impression it has been tested and proven, hence it can be said to be reliable.

The literature reviewed has shown that, good digital evidence is becoming a business enabler and therefore Digital Forensics (DF) is a vehicle that organizations use to provide good and trustworthy evidence and processes. It has also shown that enabling technology, policies, people, training/education and processes are the bedrock of the development and management of DF. From the reviewed models, we did not find any existing framework or model that covers all the key dimensions of a good digital forensics. We therefore came up with one that fits our environment. In coming up with the framework, we extracted ideas from the above reviewed models to formulate a new one, that we think will best serve Kenyan environment. Table 2.2 gives a summary of the reviewed models/Acts.

Model	Dimensions	Source
Sommer Digital Forensics model	People, Processes & Technology	Sommer, 2008
Integrated Digital Forensics in Information Assurance	People, Technology, Policies, Processes and Stages/Phases	McCumber, 2005
Legal Requirements for DF	Policies/ Processes Technology/Tools, Research, Education/Training	U.S.A undated
Cyber crime Investigation Model	Phases, Policies, Regulation, Control, Training awareness	Ciardhium 2004
DF Audit	Audit	Gordon 2006
DF E-evidence Requirements	Reliability, Relevance, Complete	Biros and Waiscr 2006
Criminal Procedure	Admissibility, Authentic, Reliable, Complete and Convincing	Evidence Act Cap 80 of 2007

Table 2.2: Summary of the Reviewed Models/Acts

CHAPTER THREE

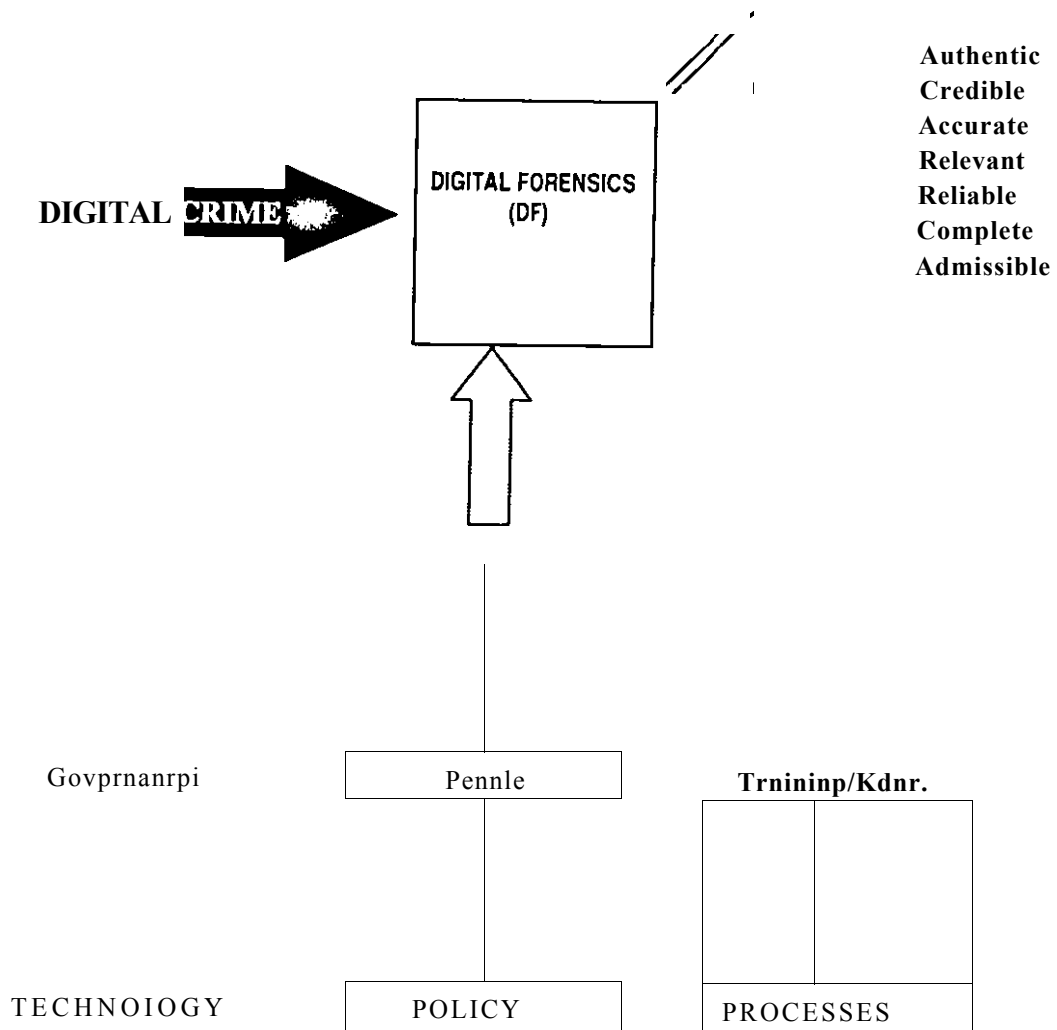
THE CONCEPTUAL FRAMEWORK

3.1 Introduction

According to Sommer (2008) & McCumber (2005), a good DF framework has three basic components namely *people*, *technology*, and *process*. It must ensure e-evidence is authentic, reliable, accurate, relevant, complete, and credible so as to be admissible before a **court**.

3.2 Deriving the Conceptual Framework

We combined research findings of Sommer (2008), McCumber (2005) and the U.S.A model (undated). They both agree on technology, regulatory policies and processes. We therefore take technology, policies and processes as the key dimensions of any DF model. These however must be resultant of some interaction of some other dimensions, like governance, training/education and people. Since in developing countries like Kenya technology, policies and governance is one of the challenges we face, we are of the view that DF must have other pillars to support them if they are to be successful. This is where we make reference to the other models discussed in chapter two. We advanced a proposition that technology, policies and processes are the dimensions whose interplay determines the governance, training/education, and staff/people on DF. The admissibility, authenticity, credibility, accuracy, relevance, reliability and completeness of digital evidence of a DF process is then determined by these six dimensions as referenced from Gordon (2006) through proper DFI processes/phases as outlined by both (Ciardhuain, S. O. 2004) and IJCSNS (2009). This is diagrammatically represented in Fig 3.1 below. In our conceptual framework, DF is creation of interplay between six dimensions. We have however categorized them into two. One category comprise of technology, regulation and processes. These dimensions must be backed by the second category namely governance, training/education and people. It is from such components that will yield the admissibility, authenticity, credibility, accuracy, relevance, reliability and completeness of digital evidence through proper phases of DFI. We wish to explain what is entailed in each of the dimensions to form the basis of examining whether necessary components of each dimension exist in our region.



30 | Page Fig. 3.1: Conceptual Framework for Digital Forensics for Kenyan Courts of Laws

3.3 Elements of the Conceptual Framework

3.3.1 Technology

No DF investigation can be conducted without a DF toolkit. Various specialized software and / or physical hardware tools will make up the DF toolkit as different tools are used for different purposes. The ways in which the tools are utilized as well as the acceptance of a specific tool by the legal authorities are vital for any forensic investigation. Although courts have found that an inanimate object, e.g. a software package cannot be considered to be an expert, the results generated by an acceptable software package are acceptable. The person who will use the software packages will have to be an expert.

3.3.2 Policy

Every organization needs policies to guide employees on activities. A general forensic investigation policy is required to provide a framework for DF policies in the organization. Examples of other policies are how to handle evidence, how to seize evidence and how to conduct covert or overt investigations. Policies are normally supported by procedures and guidelines. Procedures also need to be set up so that the investigations will be able to stand up to legal scrutiny in court. These procedures must also be scientifically sound and proven to maintain the integrity of the evidence and process. Yasinsac and Manzano (in Rawlingson, 2004) note that enterprise policies can enhance computer and network forensics. They propose six categories of policies to facilitate Digital Forensic Investigations (DFI) i.e. retaining information, planning response, training, accelerating investigation, protecting evidence and preventing anonymous activities. Well-defined policies give digital investigations and forensic examiners the authority to conduct investigations in the organization. Policies will demonstrate that an organization intends to be fair-minded and objective about how it treats employees and that it will follow due process for all investigations. The Legal and Ethical are part of policies and are very important in organizations. In Cyberspace there is no universal or common 'Cyber Law'. Various judiciary systems exist in different countries. The forensic investigator must be familiar with local legal and international laws, treaty requirements and industry specific legal requirements when preparing to present a case that will be able to stand up to legal scrutiny in-

court. The ethical aspect of DF is becoming more and more important. Although the Legal and Ethical aspects of DF have been placed together in the same dimension, it is essential to note that not all legal operations or actions are ethical. It is essential that the DF investigator does not misuse the trust that the employees place in him / her. DF investigator utilizes tools that, if handled inappropriately, can cause a lot of damage in an organization. There should be very clear guidelines on ethical behavior and possibly a code of conduct for DF Investigators to guide professional behavior.

3.3.3 Processes

According to the proposed definition, these activities are investigative in nature, and those practitioners who will employ these tools and methods will follow some form of investigative process in the performance of their duties. If properly categorized, the processes can enable practitioners to visualize where they need to add capability from what is available. Likewise, academic researchers will use the process to look for shortfalls in technology, helping them to focus on areas where research is needed the most.

3.3.4 Governance

The Corporate Governance dimension will handle the management aspects of DF in an organization. Management is responsible for the security posture of an organization. Management can only manage security incidents if for example the root cause of the event is determined and appropriate action to rectify it can be taken - this may involve forensic investigations. According to Von Solms and Louwrens (2005), IT Governance is a subset of Corporate Governance and Information Security Governance a subset of IT Governance. DF overlaps with Information Security Governance, IT governance and Corporate Governance (Von Solms & Louwrens, 2005). Forensic readiness will help to demonstrate due diligence and good corporate governance of an organization's assets (Rawlingson, 2004). It is therefore important that a forensic investigation must be performed in a way that it adds value and improves the security posture of an organization. The Corporate Governance dimension includes strategic governance and operational governance. Typically strategic governance will be from a strategic perspective, while operational governance will provide management directives on an operational level.

It is vital that management should become involved and buy into the DFMM of the organization. DF investigations can be very expensive and management must realize the need for investigations, as well as dealing with the results from an investigation. The operational governance dimension should guide the management on how to manage digital forensic investigations by providing a DFMM. This DFMM must include reactive DF as well as pro-active DF management. Pro-active DF management must ensure that all business processes are structured in such a way that essential data and evidence will be retained to ensure successful DF investigations, should an incident occur. Proper pro-active DF management should minimize interruption to the business processes while conducting an investigation. It is essential that the organization become DF ready. Re-active DF management should clearly define the management or process of an investigation, once an incident has occurred.

3.3.5 People

People are the most important part of any organization and normally the weakest link in the security chain of the organization. When an incident occurs it is most likely that people will contaminate the evidence while figuring out what has happened. Training is therefore essential. According to Rawlingson (2004) there is a huge need for forensic awareness training. This dimension will look at training and awareness programs in an organization. The profile and composition of a DF team is also very important. One person normally does not have all the required skills to conduct an investigation. It is important that digital forensics units maintain skilled, competent examiners. This can be accomplished by developing the skills of existing personnel or hiring individuals from specific disciplines. Because of the dynamic nature of the field, a comprehensive ongoing training plan should be developed based on currently available training resources and should be considered in budget submissions. Consideration may also be given to mentor programs, on-the-job training, and other forms of career development. Professional organizations such as the Information Systems Audit and Control Association (ISACA), the High Technology Crime Investigation Association (HTCIA), the Institute of Internal Auditors (IIA), the Association of Certified Fraud Examiners (ACFE) and the Information Systems Security Association (ISSA) have offered training support in this evolving area. The specialists are trained extensively on knowledge of software packages and utilities used to obtain data.

Individuals must go through rigorous training and have a solid working knowledge of the software to be competent enough to pass the test. Digital forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating. This can be attained by constructing a comprehensive training program for examiners, sound digital evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency.

3.3.6 Training/Education

It is good practice to have a dedicated internal organization or staff capacity to undertake digital evidence gathering. Forensics training and awareness on new technologies i.e tools, processes, governance, Processes-recovery, analysis, examination and presentation of e-evidence are key to DF. It is good practice to give special training to the agency's staff who practices digital evidence gathering. Computer forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating.

All the above-mentioned resources must be considered in each dimension when conducting a DF investigation or creation of DF readiness. In the Legal dimension for example, software licensing, acceptance of digital evidence in court, seizure of evidence (physical / hardware and digital), human behaviour must be incorporated. Not all the resources may exist, but all resources must be considered during an investigation. Further research is required to provide more detail regarding the resources in each dimension. The investigator will use processes and tools to deal with DF in the organization. The various dimensions will employ one or both for a successful DF investigation. The governance dimension will, for example, be implemented by using processes as well as tools to document the entire investigation. The people, legal and ethical dimensions may utilize only processes and the technology dimension would be processes as well as tools. All the dimensions interplay to give a sound DF phases and e-evidences. These dimensions are summarized in the Table 3.1 below while the developed questionnaire in appendix A and B.

Component	Description	Source
Technology	Tools (H/w, S/w) used Tested and legally accepted Proper documentation Latest technology(F-LAB) Accessibility Acceptability Security CIA information	Sommer 2008, USA undated, McCumber 2005, Director of KACC PLO Lumumba P. 2011
Training/ Education	Forensics training and awareness-on new technologies (tools, processes, governance). Processes-recovery, analysis, examination, presentation	USA undated
Policy/Legal	Policies, Guideline, Procedures, Laws, Ethics On establishing and operation of DF labs Guiding staff On DF processes On CIA of information On training Legal requirements for evidence to stand to legal scrutiny On ethics of employees not to disrupt businesses Acceptance of e-evidence in court Impact of Evidence Act 2007,Criminal Procedure Act 2008,Communication Bill 2008 be part of regulation	USA undated, Ciardhium 2004
Processes	DFI activities; Procedures to be followed; Be scientifically sound to maintain integrity of evidence; Clear processes to stand legal scrutiny.	USA, Ciardhium 2004,sommer2008
e-evidence	Authentic, admissible, complete, relevant, reliable, accurate and convincing	Gordon 2006
DF Phases	DFI stages	Ciardhium S.O 2004
People	DF team; Implements technology, processes, policies, Document processes, acquire tools Be competent team-investigators, examiners etc	Sommer 2008, McCumber 2005
Governance	Information security governance-security CIA of information. On how to be forensically ready. Operation governance -on how to manage DFI. IT governance-COBIT.	Director of KACC PLO Lumumba P. 2010

Table 3.1: The Conceptual Framework Dimensions

The literature reviewed has shown that technology, policies and processes is the environment that determines the growth of DF. It has also shown the enabling governance, staff/people and training/education as the supportive to the development and management of the DF services. There is however no available systematic research in Kenya to show the relationship between these dimensions and their influence on DF services. This research sought to explore how these factors related to DF in Kenyan. The conceptual framework is to be validated by collecting data from CID Forensics labs, KACC, PWC and High Court in an attempt to find out whether it reflects facts on the ground.

In order to examine the empirical validity of our proposed Framework for DF Services for Kenyan Courts of Laws, an exploratory survey employing different methods was conducted.

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Research Design

The research was aimed at collecting information about technology, training/education, regulatory policies, legal frameworks, governance, staff and processes as pillars of DF services. It sought to find out how the said pillars can be used to enhance DF services thus making e-evidence presented before Kenyan Courts of laws for prosecution admissible, accurate, authentic, reliable, credible and complete through proper DFI. The design of the research therefore was a survey approach. The findings of the research were used to validate the conceptual digital forensics framework for Kenyan courts of laws environment.

4.2 Target Population and Sampling Frame

This sampling method involves a random selection of particular units of the universe for constituting a sample representative of the universe (Kothari, 2008). The target population for our research was the High Court, KACC, CID and PWC. Where time and resources allow, a research should take as big a sample as possible, since this would ensure reliability of the results (Mugenda & Mugenda 2003). In most cases however, researchers have to work with a sample that is as representative as possible to ensure similar results would be obtained even when the entire population is used. The discrepancy between the sample characteristics and the population characteristics is known as sampling error. According to Mugenda & Mugenda (2003), the smaller the sample, the bigger the sampling error. It is therefore very important to identify the minimum sample size which will give results within acceptable sampling error margin. Both Mugenda & Mugenda (2003) and Kothari (2004) suggest a statistical formula for arriving at a sample size to be;

$$n = \frac{z^2}{e^*}$$

Where;

n = the desired sample size

z = the standard normal deviate at the required confidence level.

p = the proportion in the target population estimated to have characteristics being measured.

q = 1-p

e = the level of statistical significance set Kothari (2004) goes on to argue that the formula is suitable in case of infinite population in the universe.

- z is the area under the normal curve as per the table of normal curve. Given the confidence level of 95%, z is 1.96. Based on past experience and q = 1 - p. In our case, p was assumed to be 0.5 hence giving q as 0.5

- e is acceptable error ,10%

$n = 1.96^2 * 0.5 * 0.5 / 0.1^2 = 96$;

96 is the desired sample size

4.3 Research Instruments

In order to understand the research area more and in detail, the necessary data must be collected. According to Yin (2003), there are normally two types of data i.e primary and secondary data. Primary data is data that a researcher collects on her/his own for a specific purpose. When collecting data, the researcher has to choose between using question methods; like questionnaire, personal interview, using observation or documents. Documentation is mostly used to collect secondary data. Yin (2003) clearly outlines six different sources of evidence that can be used when collecting data for case study, namely: documentation; archival records; interviews; direct observation; participation and physical artifacts.

Based on the nature of our research and consideration of the above discussion, we choose to collect data and information from both primary and secondary data sources. We collected primary data through questionnaire and secondary data in terms of documentation, by gathering information from written reports, research papers, workshops proceedings and related websites. In order to collect data that is representative and reliable, four forms of data collection tools were used, namely questionnaire, interview, document study and direct observation.

4.3.1 Questionnaires

This method was used to reach a wider number of respondents from various agencies. The choice of the method was based on its wide reach, cost effectiveness, minimal biasness and anonymity which encourage respondents to give more reliable information.

Questionnaires was designed and distributed to target respondents. A pilot was done first before the final questionnaires distributed. A seven point Likert type questions was be adopted. The questionnaire largely used closed-ended questions with only a few open-ended. This is mainly to enable analysis of the data collected easier and manageable. Closed-ended questions are faster in answering and coding in statistical applications used in analyzing data. Where necessary however, open-ended questions was introduced to allow respondents to express themselves. In order to measure validity and reliability, a peer review on the instrument was conducted and there after piloting was carried out. The initial questionnaire used for piloting, returned a Cronbach alpha coefficient of between 0.4 and 0.6, which was lower than the recommended 0.7 and above. After fine tuning of the instrument, the coefficient improved to average of 0.8 which is above the minimum required of 0.7. Detailed analysis using SPSS is shown in appendix A.

4.3.2 Personal Interviews

Beside questionnaires, personal interview was conducted in the following CID departments under the in charge officers; cyber crime and investigations, documents forensic analysis, ballistics forensics, and photography. In High Court, four prosecutors were interviewed while at KACC we interviewed three officers in documents forensics lab to verify data that was collected through questionnaires and other methods. The method allowed us to probe more and deal with issues that were not dealt with by the questionnaires to get details on how they have implemented the issue of admissibility. Selection of interviewees was based on their role particularly in the field of digital evidence. This is because; they are not many to justify a survey.

4.3.3 Documents Study

To get information on existing policies, regulations, technology, governance legal and infrastructures governing digital evidence act, we studied documents available at High Court IT department particularly the grey Book and KACC library the document based forensic guide. Also existing frameworks used in other parts of the world were studied, compared with what is currently happening in Kenya from which the conceptual framework was derived.

4.3.4 Observation

We visited High Court, KACC and CID labs and analyzed the already structures and frameworks with an aim of finding out how they are structured in terms of policies, governance, standards, processes and technologies.

4.3.5 Data Analysis

According to Yin (2003), every investigation should start with a general analytic strategy, allowing the researcher to decide what to analyze and why. Once data was collected from the selected agencies, we employed SPSS, a statistical application, to analyze and draw conclusions. The findings will be used to develop a framework befitting our courts and hope it will enhance admissibility of e-evidence in our courts through strengthening policies, standards, structures, technology and infrastructures.

4.3.6 Reliability

Reliability demonstrates the extent to which the operations of a study, such as data collection procedures can be repeated with the same result (Kombo, 2006). This type of reliability is called test -retest and is time consuming (Yin, 2003). The other type of reliability test is Half-split where the result of the test is split into two halves and the coefficient of correlation is calculated and if correlation is high then it means good reliability. However according to Cronbach (1949), this test might give confusing results and as such for this research we used Cronbach alpha coefficient and not half split. It's crucial to remember that reliability is not measured but estimated (Yin, 2006). Therefore in order to measure validity and reliability, a peer review on the instrument was conducted and there after piloting was carried out

4.3.7 Validity

According to Kombo (2006), the issue concerning validity is whether the selected people who responded to the questionnaire are the ones possessing the most accurate and valuable information for the research. The researcher directly aimed law enforcement agencies like CID forensics department, ICT department of high court KACC because they are the ones who hold the required data and information with regard to the problem.

CHAPTER FIVE

FINDINGS, ANALYSIS AND INTERPRETATIONS

5.1 Introduction

The purpose of going out to collect data was to test the reliability and validity of the conceptual framework. In this chapter, we present the research findings and our interpretation from data we collected from government/private organizations practicing DF services (CID forensics labs, KACC, High Court and PWC). The findings are mainly presented using parametric statistical methods such as frequency tables, cross tabulations, regression analysis and correlation matrices.

5.2 Data Processing and Analysis

Data processing involves editing, coding, classification and tabulation of the collected raw data while analysis refers to computation of certain measures from the coded data in order to get patterns or relationship among data groups. In our survey, a total of 96 questionnaires were administered. The first step was to examine all the questionnaires in order to eliminate the incomplete and the wrongly filled ones. The elimination process left us with 80 valid questionnaires which translated to 80%.

5.2.1 Coding the Responses

In order to analyze our data using SPSS statistical software, we constructed two codebooks; one for the Kenyan Courts of laws' questionnaires (end users of DF services) and the other for KACC, PWC and CID forensics lab questionnaires (actors of DF services). For closed and Likert-type perception question, it was easy to assign numbers. For open-ended questions, especially those for High Court, we scanned through all questionnaires to identify common themes. It is from these themes that we coded the patterns.

5.2.2 Description of Reliability and Validity Testing

The first step in our data analysis was to test for the reliability and validity of our data collection instruments. In our case, the following techniques were employed:

- Reliability analysis using Cronbach Alpha
- Content validity using Factor analysis
- Face validity through peer review and experts judgment

Reliability Test

Reliability is the consistency of measurement, or the degree to which an instrument measures the same way each time it is used under the same condition with the same subjects. There are two ways that reliability is usually estimated namely *test/retest* and *internal consistency*. The idea behind test/retest is that you should get the same on several tests. On the other hand, *internal consistency* estimates reliability by grouping questions in a questionnaire that measure the *same concept*

Validity Test

Validity refers to the best available approximation to the truth or falsity of a given inference, proposition or conclusion. Three commonly used validity testing techniques are construct, content and face validity. **Construct Validity** refers to the totality of evidence about whether a particular operationalization of a construct adequately represents what is intended by theoretical account of the construct being measured. Such lines of evidence include statistical analyses of the internal structure of the test including the relationships between responses to different test items. **Content Validity** is a non-statistical type of validity that involves the systematic examination of the test content to determine whether it covers a representative sample of the behaviour domain. Such validity testing is done by a panel of experts who review the specifications of selected items. Through their recommendation, the content validity of a test can be improved.

Face Validity is also a non-statistical validation method used to get opinions on whether an instrument "looks like" it is going to measure what it is supposed to measure.

While content validity requires more rigorous analysis by subject experts, face validity only requires an intuitive judgment. In order to investigate the face validity of our research instruments, the two sets of questionnaires were given out to technical and non technical people to check on whether the questions were clear and in line with our research questions addressed by the proposed framework. Based on reviewers' comments, necessary changes were made before the questionnaires were administered. Therefore, these test results demonstrate that the two questionnaires used to test reliability and validity of the proposed framework is valid. Consequently, the responses obtained from the respondents are valid.

5.2.3 Reliability Analysis of the Collected Data

The most immediate analysis we carried out was the reliability analysis on *Likert-type perception questions*. This was aimed at establishing whether our revised questionnaires met the proposed minimum Cronbach Alpha coefficient. Using this method, the minimum proposed coefficient is 0.7. The closer the coefficient is to 1, the better, meaning the tool's reliability is good. The sample SPSS test output shown in Figure 5.1 shows that our tool was reliable because the Cronbach alpha is 0.8350 while the correlation matrix showed values greater than the recommended 0.3. Therefore the results demonstrate that our questionnaires are reliable measurement instruments. Below are sample SPSS test output showing the reliability test obtained.

```

***** Method 1 (space saver) will be used for this analysis *****
  R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   ( A L P H A )
Item-total Statistics
      Scale          Scale          Corrected          Alpha
      Mean          Variance        Item-          if Item
      if Item      if Item        Total          if Item
      Deleted      Deleted        Correlation    Deleted

T1      186.8625      2641.5378      .5673      .8293
T2      187.9750      2636.5563      .4840      .8295
T3      187.7125      2635.3467      .6163      .8288
T4      186.6500      2612.1544      .7695      .8270
T5      187.2625      2615.1074      .7802      .8271
T6      189.1875      2684.9138      .2733      .8328
PP1     187.4625      2656.4543      .5870      .8301
PP2     188.1250      2661.5791      .4785      .8307
PP3     186.7000      2622.4405      .7929      .8276
TE1     186.4875      2638.6074      .6524      .8289
TE2     187.4500      2642.0481      .6085      .8292
TE3     187.4750      2624.8095      .7428      .8278
TE4     186.5125      2425.0884      .3096      .8391
TE5     187.3000      2645.7063      .6481      .8293
PR1     187.1125      2651.1138      .6834      .8295
PR2     187.0875      2646.1821      .6366      .8294
PR3     186.9625      2639.5302      .6478      .8289
PR4     186.9750      2628.3032      .7101      .8281
PR5     186.6500      2618.9139      .7142      .8275
G1      187.5000      2662.8101      .5047      .8307
G2      187.6375      2662.6391      .5278      .8306
G3      187.0875      2596.4606      .7228      .8262
G4      184.2625      2351.9176      .1495      .8872
G5      186.7000      2620.0861      .7321      .8276
G6      186.1375      2568.3479      .2506      .8353
G7      186.7625      2607.6771      .7418      .8268
LI      187.9500      2636.5038      .5701      .8290
L2      185.9250      2676.3234      .0420      .8461
L3      187.3250      2409.0070      .3190      .8392
L4      187.3750      2593.1234      .7108      .8261
L5      187.2250      2611.5690      .6551      .8273
L6      186.9375      2599.1479      .7345      .8263
L7      186.5875      2609.5112      .7572      .8269
EDI     186.5625      2615.4138      .7663      .8272
ED2     186.9250      2611.6652      .7641      .8270
ED3     186.8125      2610.9897      .7340      .8270
ED4     186.4000      2563.3570      .3114      .8319

  R E L I A B I L I T Y   A N A L Y S I S   -   S C A L E   ( A L P H A )
Reliability Coefficients
N of Cases      80.0      N of Items = 38
Alpha =      8350

```

Fig 5.1: Reliability Analysis of the Kenyan Courts Questionnaires

```

**** Method 2 (covariance matrix) will be used for this
REL I A B I L I T Y   A N A L Y S I S   -   S C A L E   ( A L P H A )

```

		Mean	Std Dev	Cases
1.	T1	5.3000	1.7018	80.0
2.	T2	3.1500	2.0629	80.0
3.	T3	4.4500	1.6680	80.0
4.	T4	5.5125	1.6381	80.0
5.	T5	4.9000	1.5799	80.0

Correlation Matrix

	T1	T2	T3	T4	T5
T1	1.0000				
T2	.1067	1.0000			
T3	.2774	.2744	1.0000		
T4	.5117	.0043	.4241	1.0000	
T5	.3691	.1445	.4976	.8075	1.0000

N of Cases = 80.0

Statistics for Scale	Mean	Variance	Std Dev	N of Variables
	23.3125	32.6986	5.7183	5

Item--total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Alpha Item Deleted
T1	18.0125	24.1391	.3387	.2893	.6585
T2	20.1625	26.3910	.0968	.1380	.7848
T3	18.8625	21.5125	.5431	.3098	.5690
T4	17.8000	20.6937	.6255	.7124	.5324
T5	18.4125	20.4733	.6805	.6940	.5116

Reliability Coefficients 5 items

Alpha	.8432	Standardized item alpha	.8467
-------	-------	-------------------------	-------

Fig 5. 2: Reliability Analysis of the CIO Forensics Lab Questionnaire

5.2.4 Validity Analysis of the Collected Data

In order to further assess the convergent and discriminant validity of our test instruments, factor analyses were performed. Factor Analysis is a statistical measure that used to analyze the interrelationships among a large number of variables and explain the variables in terms of (heir common underlying dimensions. If the dimensions are indeed distinct one would expect to find factors with similar items loading together to form a coherent structure. In our study, a factor analysis for each questionnaire items was generated using Principle Components extraction and varimax rotation. Figure 5.3 shows the sample Kaiser-Meyer-Oklin (KMO) test result of 0.754 above the minimum KMO of 0.60. The Bartlett's Test of Significance 0.000 which is less than the set maximum of 0.5.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.754
Bartlett's Test of Sphericity	Approx. Chi-Square	341.750
	df	36
	Sig.	.000

Fig 5. 3: KMO and Bartlett's test

5.3 Detailed Analysis of Responses Questionnaire

In this section, a detailed analysis of the responses obtained from CID DF forensics labs, KACC, Kenya High court and PWC that should represent the Kenyan players in DF is given. To make the data representative, the target group was segmented according to gender, age, level of education and income levels to take care of various interests in the DF world. Below is more detailed analysis.

5.3.1 Demographic Analysis of the Respondents

Gender

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid male	60	75.0	75.0	75.0
female	20	25.0	25.0	100.0
Total	80	100.0	100.0	

Table 5.1: Gender Distribution

The distribution of questionnaires was balanced on the gender, but male respondents were more than female respondents. This perhaps is an indication that the field of DF requires men than women due to the nature of work. The representation based on gender is however not the subject of the research.

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	below 30	26	32.5	32.5	32.5
	31-50	47	58.8	58.8	91.3
	above 50	7	8.8	8.8	100.0
	Total	80	100.0	100.0	

Table 5. 2: Age Distribution

It is our considered view that people of different age groups embrace DF differently. The distribution therefore tried to capture adults of various age groups. Majority however were between 31 and 50 years. This is actually justified since the field of DF is still young in our country Kenya and again the fact that many cases of Digital crime involves people of around that age.

Education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	15	18.8	18.8	18.8
	Degree	54	67.5	67.5	86.3
	Masters	11	13.8	13.8	100.0
	Total	80	100.0	100.0	

Table 5. 3: Education Level Distribution

The respondents also represented all levels of education meaning the findings from the data are not skewed in relation to education status. Majority of the respondents were however holders of degree. We can infer that the field of DF requires people with skills.

Income

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	<20000	2	2.5	2.5	2.5
	21,000-50,000	54	67.5	67.5	70.0
	>50,000	24	30.0	30.0	100.0
	Total	80	100.0	100.0	

Table S. 4: Income Level Distribution

The respondents also represent a varied income levels and we sought to establish how this variable affects staff. The data indicates more than 70% earn KSh. 50,000 and below per month. This can be interpreted to mean that we are yet to pay well the staff in the DF field and perhaps the reason why we lack enough trained and qualified staff.

5.3.2 Years of Experience in DF

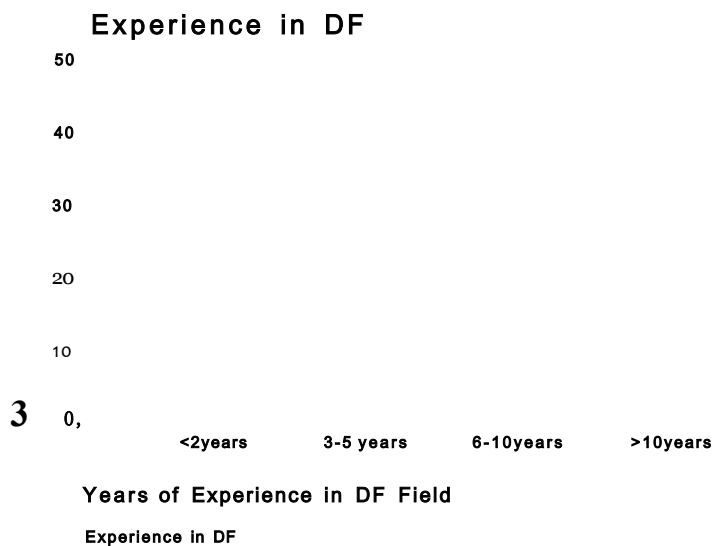


Fig 5.4: Rating of experience in DF field.

It is our considered view that experience affects DF services. The distribution therefore tried to capture years of experience in the field of DF. Majority had an experience of 3-5 years. This may be an indicator that the field of DF is still young in our country Kenya.

5.3.3 Inferential Analysis

5.3.3.1 Technology

It has already been shown in the literature reviewed that technology is the bedrock of digital forensics. The research sought to establish whether Kenya has access to technology on which DF can thrive and how participants were using the technology in relation to DF. We specifically sought to ascertain the availability and use of modern technology in DF and whether it impacts DF processes. The research shows majority of respondents agree that we don't have the modern and well equipped lab to handle DF processes.

In other words technologically we are poor. The survey found out 60% of the respondents considers we do not have modern and well equipped DF lab to handle DF successfully. It was also established that 77% of respondents agree that technology has a high impact on the reliability of DF services. This is a good indicator that we need to establish sound DF labs with latest technology to cope up with the growing rate of e-crime and produce forensically sound evidence.

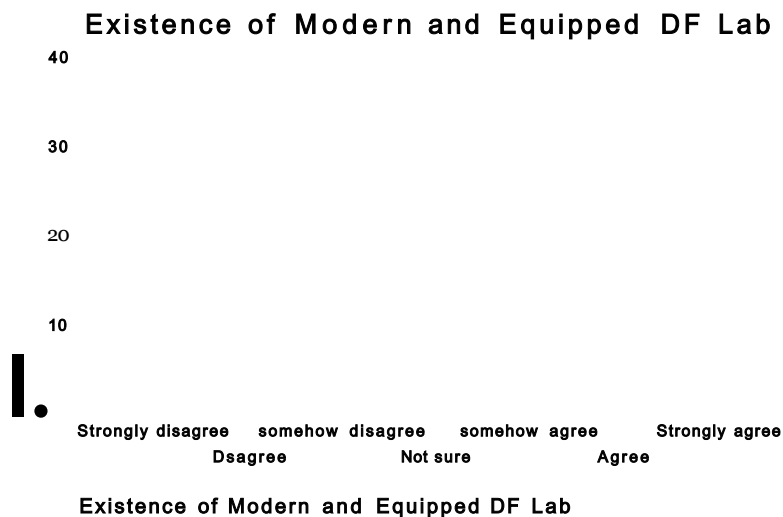


Fig 5. 5: Existence of Modern and Equipped DF Lab

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	28	35.0	35.0	35.0
	Disagree	11	13.8	13.8	48.8
	somehow disagree	9	11.3	11.3	60.0
	Not sure	4	5.0	5.0	65.0
	somehow agree	11	13.8	13.8	78.8
	Agree	15	18.8	18.8	97.5
	Strongly agree	2	2.5	2.5	100.0
	Total	80	100.0	100.0	

Table 5. 5: Existence of Modern and Equipped DF Lab

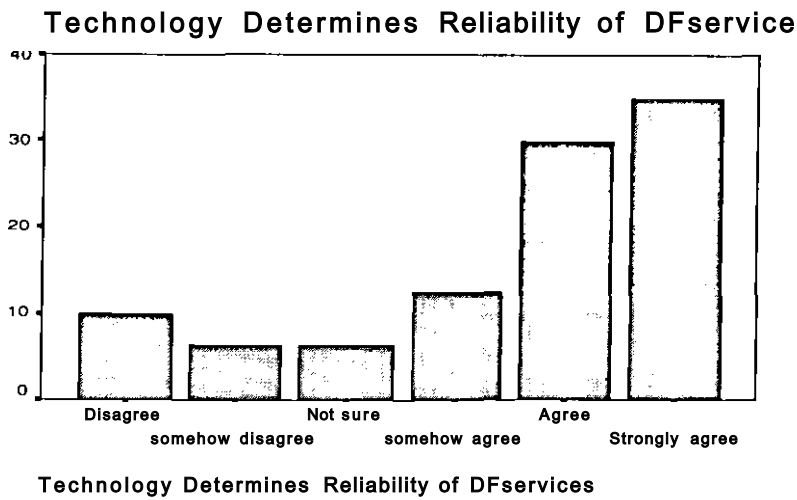


Fig 5. 6: Technology Determines Reliability of DF services

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	8	10.0	10.0	10.0
	somehow disagree	5	6.3	6.3	16.3
	Not sure	5	6.3	6.3	22.5
	somehow agree	10	12.5	12.5	35.0
	Agree	24	30.0	30.0	65.0
	Strongly agree	38	35.0	35.0	100.0
	Total	80	100.0	100.0	

Table 5.6: Technology Determines Reliability of DF services

To assess whether technology component has impact on the reliability of DF services, we did correlation analysis. To interpret the strength of relationship from the value of Pearson correlation (r), we adopted Cohen (1988) guidelines. The author suggests absolute value of r in the range of 0.10 to 0.29 represent small strength, 0.30 to 0.49 is medium while 0.50 to 1.0 is large. From the correlations shown in the table below, there is positive relationship between technology and DF services.

		Use of tested and legally okayed tools	Existence of Modern and Equipped DF Lab	Availability of latest tools use	Technology Determines Reliability of DF services	Technology used comply with legal and ethics requirements	Inclusive technology use
Use of tested and legally okayed tools	Pearson Correlation	1	.734(")	.4770	.512(**)	.369(")	.064
	Sig. (2-tailed) N	80	.346 80	.013 80	.000 80	.001 80	.575 80
Existence of Modern and Equipped DF Lab	Pearson Correlation	.734(")	1	-.2740	.564(")	.144	.143
	Sig. (2-tailed) N	.346 80	.014 80	.970 80	.201 80	.205 80	.205 80
Availability of latest tools use	Pearson Correlation	.477(*)	.2740	1	.424(")	.498(")	.535(")
	Sig. (2-tailed) N	.013 80	.014 80	.000 80	.000 80	.000 80	.000 80
Technology Determines Reliability of DF services	Pearson Correlation	.512(**)	.564(")	.424(")	1	.8070)	.100
	Sig. (2-tailed) N	.000 80	.970 80	.000 80	.000 80	.000 80	.380 80
Technology used comply with legal and ethics requirements	Pearson Correlation	.369(")	.144	.498(**)	.807n	1	.403(")
	Sig. (2-tailed) N	.001 80	.201 80	.000 80	.000 80	.000 80	.000 80
Inclusive technology use	Pearson Correlation	.064	.143	.535(")	.100	.4030)	1
	Sig. (2-tailed) N	.575 80	.205 80	.000 80	.380 80	.000 80	.000 80

*1 Correlation is significant at the 0.01 level (2-tailed).

Table 5.7: Technology and DF Services Correlation

From the above table we can infer that technology has a correlation with the availability of well equipped modern lab, all round technology, legally acceptable and soundness of DF services. There is need therefore to set up modern well equipped DF labs to achieve forensically sound processes.

5.3.3.2 Training/Education

Lack of training and awareness on DF has already being cited as one of the major challenges facing DF in Kenya. We sought to find out if indeed we have enough trained and qualified DF staff, whether training is a key component of DF and if we have regular of such training. Majority (at 67 %) agree that there is no enough trained and qualified staff on DF. On regular training 72 % agree that regular training and awareness on DF is missing. However despite this, 81 % agree that training is a key component to DF services. This explains why we still lag behind in DF. There is need therefore for training and awareness of staff on DF issues.

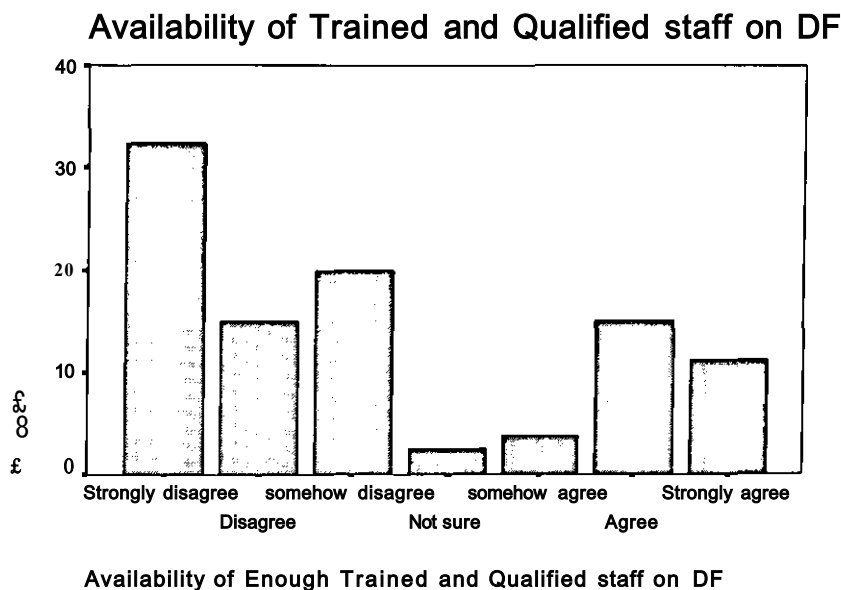


Fig 5. 7: Availability of Enough Trained and Qualified staff on DF

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	26	32.5	32.5	32.5
	Disagree	12	15.0	15.0	47.5
	somehow disagree	16	20.0	20.0	67.5
	Not sure	2	2.5	2.5	70.0
	somehow agree	3	3.8	3.8	73.8
	Agree	12	15.0	15.0	88.8
	Strongly agree	9	11.3	11.3	100.0
	Total	80	100.0	100.0	

Table 5. 8: Availability of Enough Trained and Qualified Staff on DF

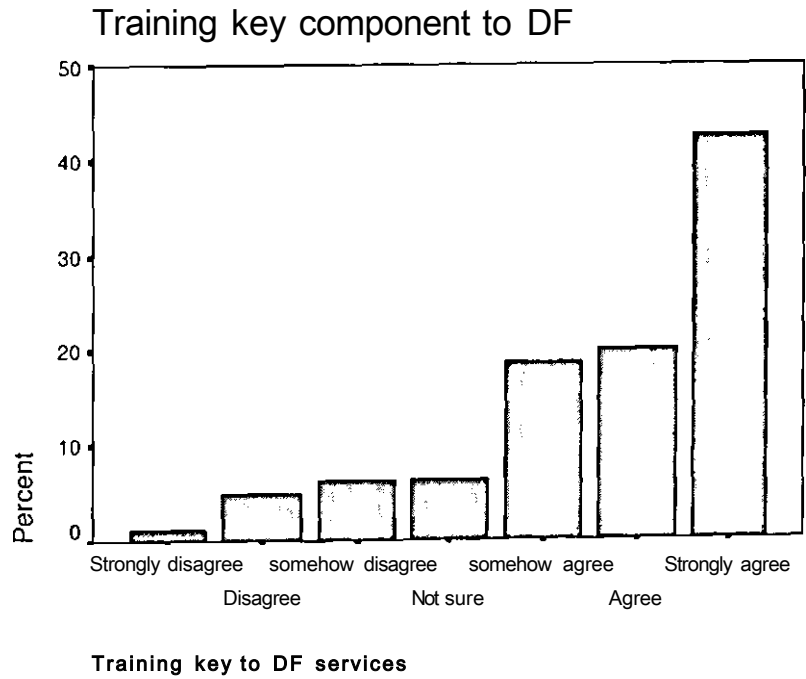
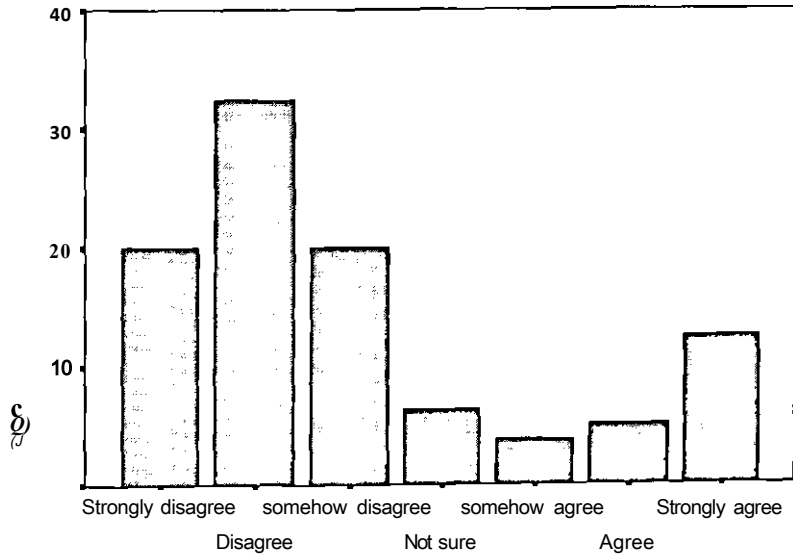


Fig 5. 8: Training key to DF services

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	1	1.3	1.3	1.3
	Disagree	4	5.0	5.0	6.3
	somehow disagree	5	6.3	6.3	12.5
	Not sure	5	6.3	6.3	18.8
	somehow agree	15	18.8	18.8	37.5
	Agree	16	20.0	20.0	57.5
	Strongly agree	34	42.5	42.5	100.0
	Total	80	100.0	100.0	

Table 5. 9: Training Key to DF Services

Training and Awareness of staff on DF issues



Regular training and awareness of staff on DF issues

Fig 5. 9: Regular training and awareness of staff on DF issues

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	16	20.0	20.0	20.0
	Disagree	26	32.5	32.5	52.5
	somehow disagree	16	20.0	20.0	72.5
	Not sure	5	6.3	6.3	78.8
	somehow agree	3	3.8	3.8	82.5
	Agree	4	5.0	5.0	87.5
	Strongly agree	10	12.5	12.5	100.0
	Total	80	100.0	100.0	

Table 5.10: Regular Training and Awareness of Staff on DF Issues

		Mean	Std Dev	Cases
1.	TE1	5.4799	1.8049	80
2.	TE2	5.9484	1.6768	80

Correlation Matrix		
	TE1	TE2
TE1	1.0000	
TE2	.5798	1.0000

N of Cases =	80
--------------	----

Table 5.11: Correlations for Training/Education

The means of the test items of the construct of technology indicate that generally, the respondents are aware that there is no adequate trained and qualified staff on DF, regular training and awareness is lacking. There is a significant correlation of 0.5798 between the two test items under the construct of training.

		Training key to DF services	Regular training and awareness of staff on DF issues	Training of staff on new technologies, tools, regulations	Competence of staff determines authenticity of evidence
Training key to DF services	Pearson Correlation	1	.172	.499(")	.873(")
	Sig. (2-tailed)		.127	.000	.000
	N	80	80	80	80
Regular training and a awareness of staff on DF issues	Pearson Correlation	.172	1	.395{")	.127
	Sig. (2-tailed)	.127		.000	.263
	N	80	80	80	80
Training of staff on new technologies, tools, regulations	Pearson Correlation	.499(**)	.395{")	1	.578{")
	Sig. (2-tailed)	.000	.000		.000
	N	80	80	80	80
Competence of staff determines authenticity of evidence	Pearson Correlation	.873(**)	.127	.578{")	1
	Sig. (2-tailed)	.000	.263	.000	
	N	80	80	80	80

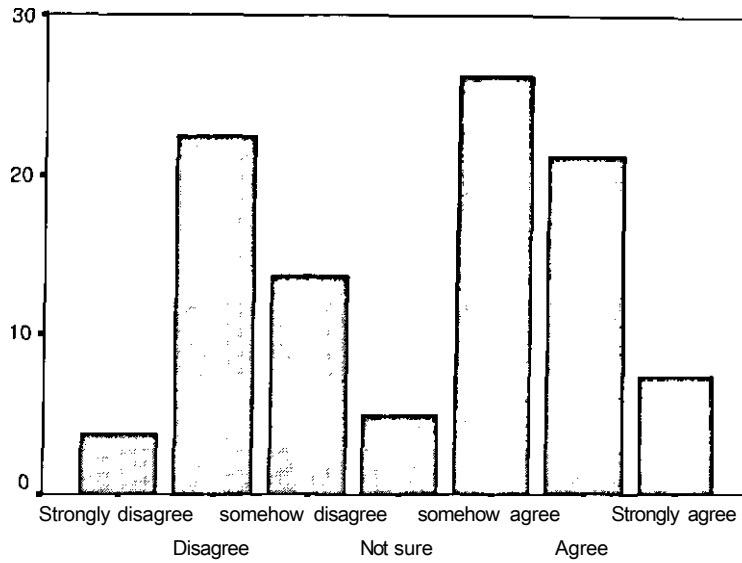
" Correlation is significant at the 0.01 level (2-tailed).

Table 5.12: Correlations for Training/Education with DF

5.3.3.3 Policy and Legal Dimension

The research findings mixed reactions in terms of DF legal awareness. However majority (56%) agree that they are aware of the DF legal systems in place. However, there is a perception that the current law and policies are not adequate to deal with challenges of DF. It was noted that a total of 67.0% agree that should a good legal framework be put in place, it would enhance DF processes. The table 5.13 below gives a summary of our finding.

DF Legal Awareness



DF Legal and ethical, policies & procedures awareness

Fig 5.10: DF Legal and ethical, policies & procedures awareness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	3	3.8	3.8	3.8
	Disagree	18	22.5	22.5	26.3
	somehow disagree	11	13.8	13.8	40.0
	Not sure	4	5.0	5.0	45.0
	somehow agree	21	26.3	26.3	71.3
	Agree	17	21.3	21.3	92.5
	Strongly agree	6	7.5	7.5	100.0
	Total	80	100.0	100.0	

Table 5.13: DF Legal and Ethical, Policies & Procedures Awareness

Current legal/policies on DF

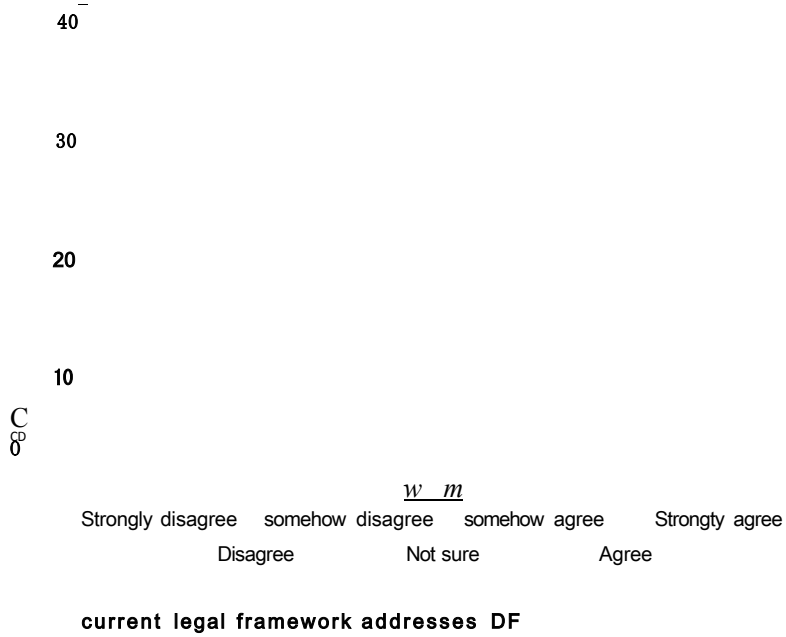


Fig 5.11: Current legal framework addresses DF

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	7	8.8	8.8	8.8
	Disagree	27	33.8	33.8	42.5
	somehow disagree	10	12.5	12.5	55.0
	Not sure	2	2.5	2.5	57.5
	somehow agree	9	11.3	11.3	68.8
	Agree	23	28.8	28.8	97.5
	Strongly agree	2	2.5	2.5	100.0
	Total	80	100.0	100.0	

Table 5.14: Current Legal Framework Addresses DF

Good Legal Framework Enhances DF

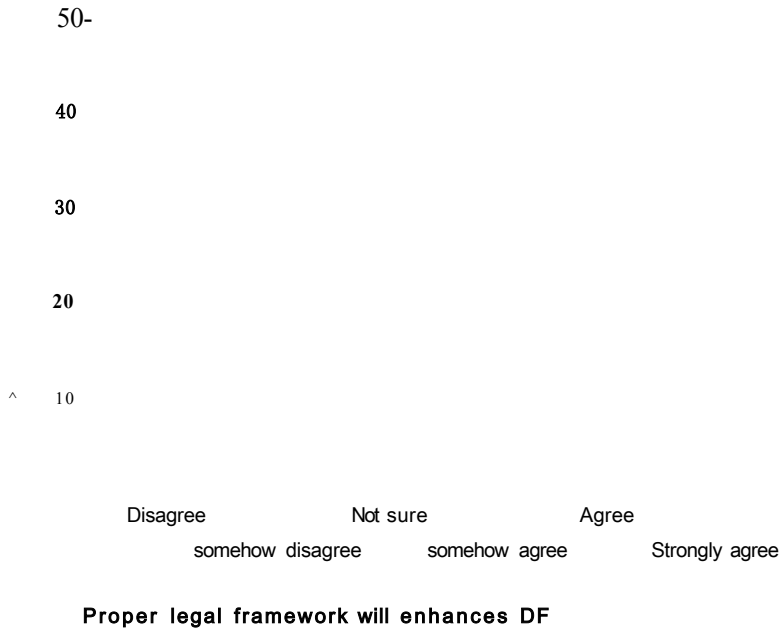


Fig 5.12: Proper legal framework will enhances OF

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Disagree	8	10.0	10.0	10.0
somehow disagree	5	6.3	6.3	16.3
Not sure	5	6.3	6.3	22.5
somehow agree	13	16.3	16.3	38.8
Agree	13	16.3	16.3	55.0
Strongly agree	36	45.0	45.0	100.0
Total	80	100.0	100.0	

Table 5.15: Proper Legal Framework will Enhances DF

		Mean	Std Dev	Cases
1.	LI	3.4933	2.1597	80.0
7.	L7	3.3098	2.2582	80.0

Correlation Matrix		
	LI	L7
LI	1.0000	
L7	.5134	1.0000

N of Cases =	80.0
--------------	------

Table 5.16: Correlations for Legal and Policies

The means of legislation of proper Laws on policies and processes implies that the e-evidence from such processes of DF will be authentic hence admissible. The correlation between the test items for legal is a significant 0.5134.

Correlations

		Proper legal framework will enhances DF	current legal framework addresses DF	DF Legal and ethical, policies & procedures awareness
Proper legal framework will enhances DF	Pearson Correlation	1	.567	.6860
	Stg. (2-tailed)		.557	.010
	N	80	80	80
current legal framework addresses DF	Pearson Correlation	.567	1	.441 (")
	Sig. (2-tailed)	.557		.000
	N	80	80	80
DF Legal and ethical, policies & procedures awareness	Pearson Correlation	.686(4)	4 4 i n	1
	Sig. (2-tailed)	.010	.000	
	N	80	80	80

* Correlation is significant at the 0.05 level (2-tailed).

" Correlation is significant at the 0.01 level (2-tailed).

Table S. 17: Correlations for Legal and Policies with DF

From the above table we can infer that the availability of proper legal framework and awareness of the same means authenticity of DF services.

There is need therefore to create establish and create awareness of proper legal framework on DF.

5.33.4 Governance

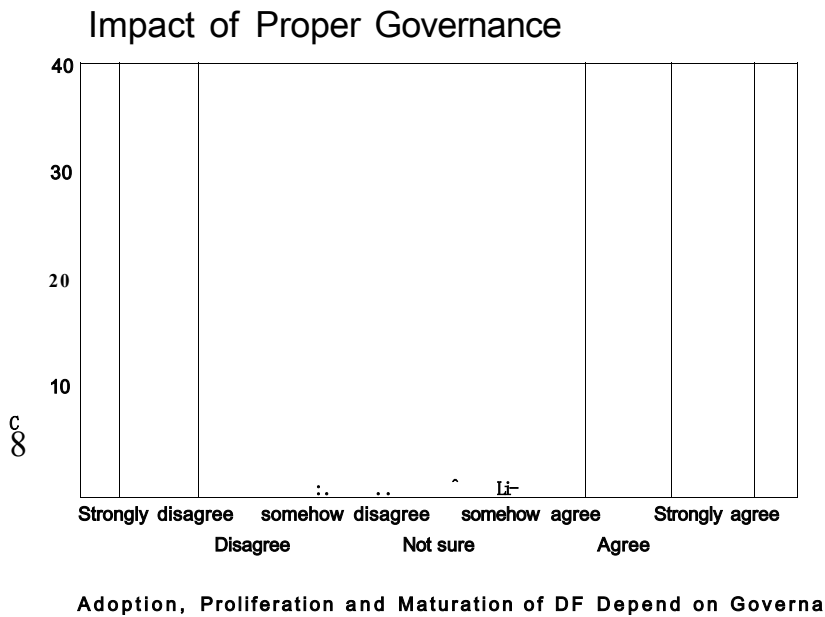


Fig 5.13: Adoption, Proliferation and Maturation of DF Depend on Governance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	11	13.8	13.8	13.8
	Disagree	2	2.5	2.5	16.3
	somehow disagree	5	6.3	6.3	22.5
	Not sure	4	5.0	5.0	27.5
	somehow agree	8	10.0	10.0	37.5
	Agree	30	37.5	37.5	75.0
	Strongly agree	20	25.0	25.0	100.0
	Total	80	100.0	100.0	

Table 5.18: Adoption, Proliferation and Maturation of DF Depend on Governance

Correlations

		Mean	Std Dev	Cases
1.	G1	5.0344	1.9055	80
2.	G2	4.8317	1.9726	80
3.	G3	3.9618	1.9095	80

Correlation Matrix			
	G1	G2	G3
G1	1.0000		
G2	.7013	1.0000	
G3	.4805	.5333	1.0000

N of Cases =	80
--------------	----

Table 5.19: Correlations for Governance

The means for the test items for governance on DF show that the adoption, proliferation and maturation of DF depend on the governance in place. Most of the responded (67%) agree with the notion that governance as a component enhances DF services. The correlations between the test items were significant with all having a value of above 0.3.

		Adoption, Proliferation and Maturation of DF Depend on Governance	Good governance boost DF staff	Governance means proper legal in place	Good govern leads to reliable evidence
Adoption, Proliferation and Maturation of DF Depend on Governance	Pearson Correlation	1	.705(*)	.565	.615
	Sig. (2-tailed)		.006	.144	.056
	N	80	80	80	80
Good governance boost DF staff	Pearson Correlation	.705(*)	1	.543D	.703(**)
	Sig. (2-tailed)	.006		.030	.000
	N	80	80	80	80
Governance means proper legal in place	Pearson Correlation	.565	.543(**)	1	.545
	Sig. (2-tailed)	.144	.030		.692
	N	80	80	80	80
Good govern leads to reliable evidence	Pearson Correlation	.615	.703(*)	.045	1
	Sig. (2-tailed)	.056	.000	.692	
	N	80	80	80	80

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Table 5.20: Correlations for Governance with DF

Clearly there is a very strong positive relationship between governance and the Adoption, Proliferation and Maturation of DF. Likewise, if there proper governance it translates to reliability of DF services. This validates our preposition that governance plays an important role in enhancing DF services in developing countries like Kenya.

5.3.3.5 Processes

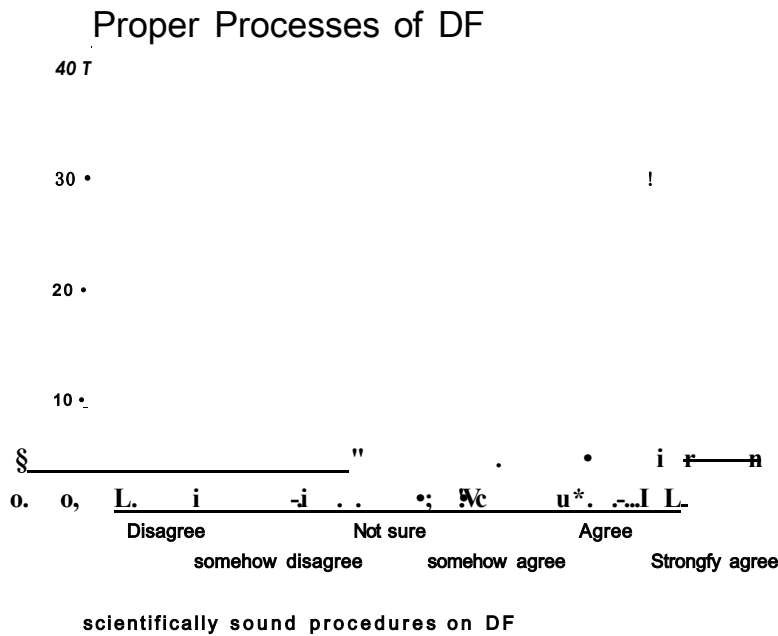
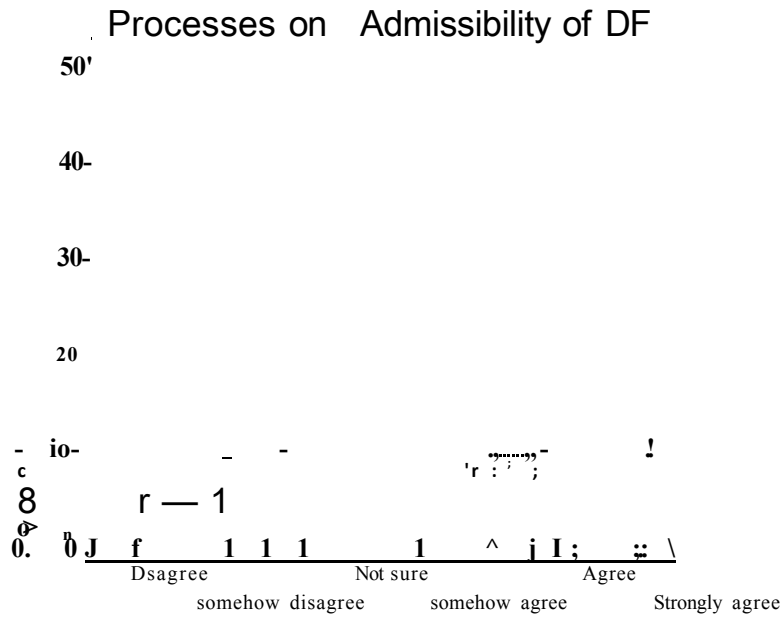


Fig 5.14: Scientifically sound procedures on DF

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	30	37.5	37.5	37.5
	somehow disagree	3	3.8	3.8	41.3
	Not sure	6	7.5	7.5	48.8
	somehow agree	7	8.8	8.8	57.5
	Agree	30	37.5	37.5	95.0
	Strongly agree	4	5.0	5.0	100.0
	Total	80	100.0	100.0	

Table 5.21: Scientifically Sound Procedures on DF



Good processes guarantee admissibility of DF

Fig 5.15: Good processes guarantee admissibility of DF

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	5	6.3	6.3	6.3
	somehow disagree	11	13.8	13.8	20.0
	Not sure	5	6.3	6.3	26.3
	somehow agree	8	10.0	10.0	36.3
	Agree	19	23.8	23.8	60.0
	Strongly agree	32	40.0	40.0	100.0
	Total	80	100.0	100.0	

Table 5. 22: Good Processes Guarantee Admissibility of OF

Correlations

		Mean	Std Dev	Cases
1.	PR1	4.4551	2.0113	80
2.	PR2	4.5124	2.0401	80
3.	PR3	4.4704	1.9585	80
4.	PR4	4.3748	1.9271	80
5.	PR5	4.7916	2.0428	80
6.	PR6	4.8604	1.9705	80

Correlation Matrix					
	PR1	PR2	PR3	PR4	PR5
PR1	1.0000				
PR2	.5855	1.0000			
PR3	.6799	.8169	1.0000		
PR4	.6187	.5840	.6120	1.0000	
PR5	.5509	.4486	.4708	.5800	1.0000
PR6	.5052	.4758	.4653	.5541	.8004

	PT6
PT6	1.0000

N of Cases = 80

Table 5.23: Correlation for Processes

The construct of processes had six test items. On average, the respondents neither agreed nor disagreed that processes is in place. However majority (73%) agree that good processes enhances admissibility of DF services. The correlations between the test items were significant with all having a value of above 0.3.

		Use of well developed processes on DF	Scientifically sound procedures on DF	Clear procedures and guidelines on processes	Processes comply with legal and industry demands on DF	Good processes guarantee admissibility of DF
Use of well developed processes on DF	Pearson Correlation	1	.717(")	.8020	.7600	.740(")
	Sig. (2-tailed)		.004	.000	.000	.000
	N	80	80	80	80	80
Scientifically sound procedures on DF	Pearson Correlation	.717(")	1	.6450	.584(")	.540(")
	Sig. (2-tailed)	.004		.002	.000	.002
	N	80	80	80	80	80
Clear procedures and guidelines on processes	Pearson Correlation	.8020	.645(")	1	.8960	.7030
	Sig. (2-tailed)	.000	.002		.000	.000
	N	80	80	80	80	80
Processes comply with legal and industry demands on DF	Pearson Correlation	.7600	.584H	.896(")	1	.7840
	Sig. (2-tailed)	.000	.000	.000		.000
	N	80	80	80	80	80
Good processes guarantee admissibility of DF	Pearson Correlation	.7400	.5400	.703D	.784(")	1
	Sig. (2-tailed)	.000	.002	.000	.000	
	N	80	80	80	80	80

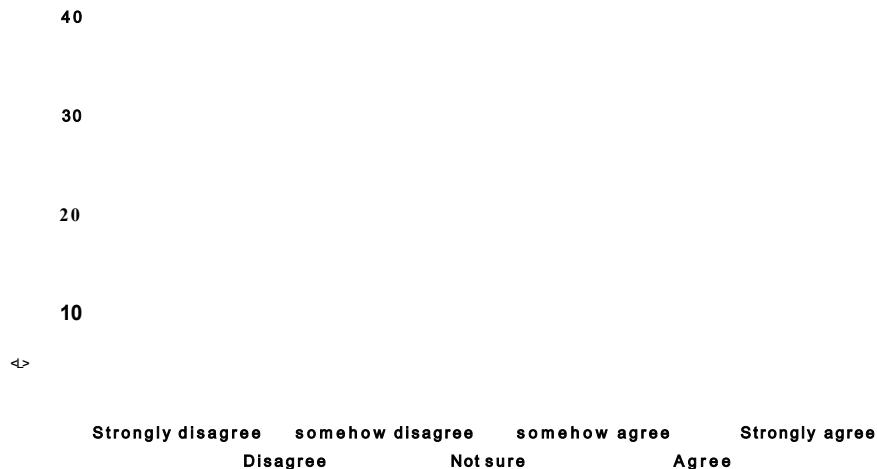
" Correlation is significant at the 0.01 level (2-tailed).

Table 5. 24: Correlation for Processes with DF

Obviously there is a strong positive relation between availability of forensically sound processes and admissibility of outcome of the DF services. There is also a significant positive relationship between scientifically sound procedures and meeting demands of the industry of the same. We can conclude therefore, the presence of good sound DF processes mean admissibility of DF services.

5.3.4.6 People

The impact of trained staff/people in DF



People are the most important part of any organization and normally the weakest link in the security chain of the organization. When an incident occurs it is most likely that people will contaminate the evidence while figuring out what has happened. Training is therefore essential. The profile and composition of a DF team is also very important. One person normally does not have all the required skills to conduct an investigation. It is important that digital forensics units maintain skilled, competent examiners. This can be accomplished by developing the skills of existing personnel or hiring individuals from specific disciplines. Because of the dynamic nature of the field, a comprehensive ongoing training plan should be developed based on currently available training resources and should be considered in budget submissions. Consideration may also be given to mentor programs, on-the-job training, and other forms of career development. The specialists are trained extensively on knowledge of software packages and utilities used to obtain data. Individuals must go through rigorous training and have a solid working knowledge of the software to be competent enough to pass the test. Digital forensics as a discipline demands specially trained personnel, support from management, and the necessary funding to keep a unit operating. This can be attained by constructing a comprehensive training program for examiners, sound digital evidence recovery techniques, and a commitment to keep any developed unit operating at maximum efficiency. The findings indicate that 75% of the respondents agree that the quality of staff is key to DF.

CHAPTER SIX

THE VALIDATED FRAMEWORK

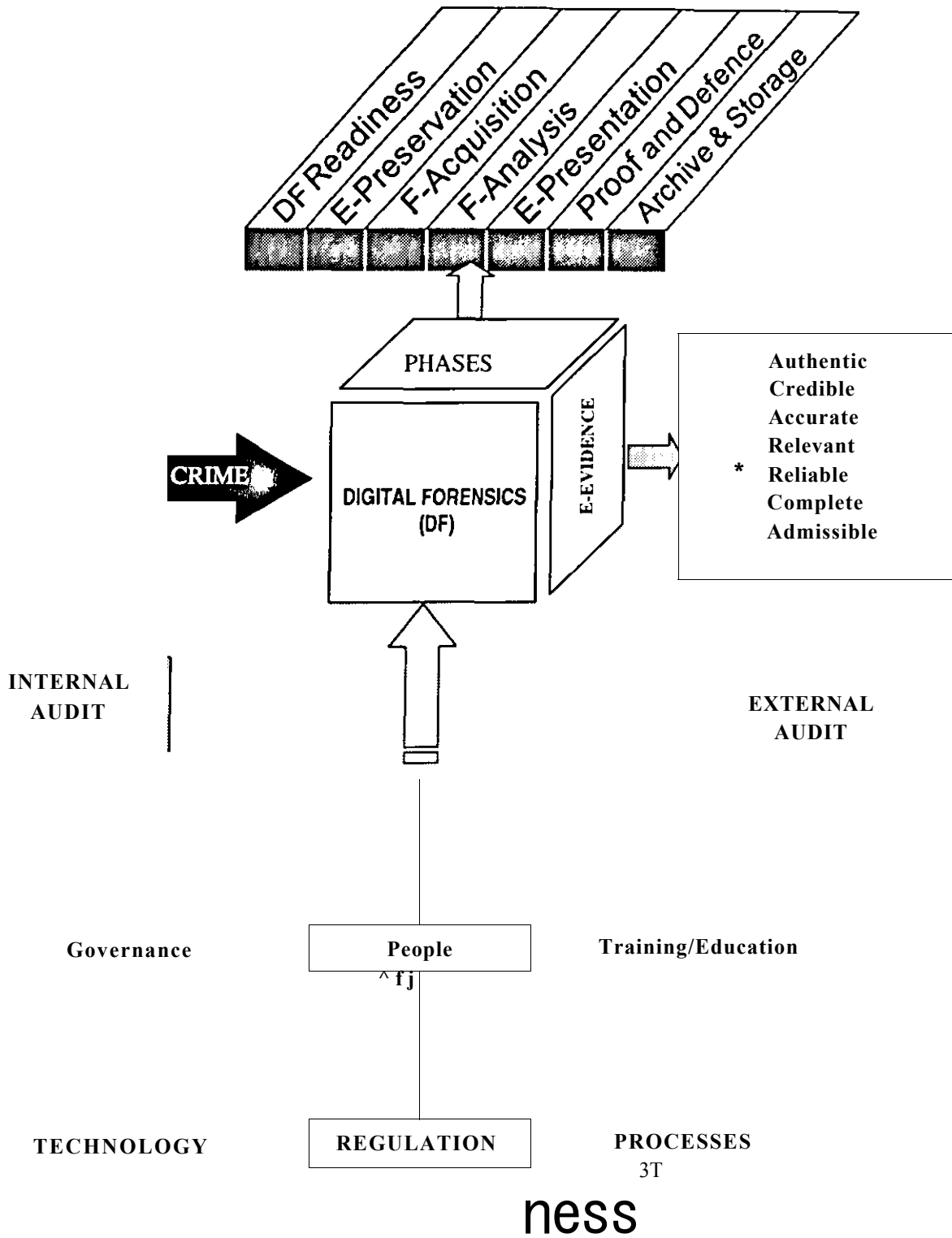
6.1 Introduction

This chapter contains the discussions on framework validation. In chapter three section a conceptual draft framework consisting of six dimensions of DF namely technology, regulation, people, governance, training/education and processes was proposed. To validate the framework, we went into the field to collect data from the following sources:

1. Kenya High Court
2. CID Digital Forensics Labs
- 3. KACC**
- 4. PWC**

6.2 Validated Framework

The finding of the research validated the framework that was proposed. The Framework is however refined by DF awareness and Audit components that came out very strongly as an important factor in making impact of the DF dimensions felt. Further, it was established the term 'Policy' is not legally binding, and hence was changed to 'Regulation' which encompasses both law and policies. The validated digital forensics framework is therefore as shown in Fig 6.1 below. The DF awareness on these dimensions is expected to unlock the potential of DF in Kenya. The government needs to heighten campaign on DF awareness for the success of DF services. Similarly, auditing of the DF services is critical to admissibility of DF evidence presented before a court of law. Both the government and private agencies practicing DF services should consider auditing their services to make the process authentic. Greater DF awareness and Auditing is expected to improve e-evidence in terms of authenticity, credibility, accuracy, reliability, completeness and above all the admissibility of evidence. Table 6.1 Summary of dimensions for the Validated Framework



69 | Page Fig.6.1: Validated Conceptual Framework for Digital Forensics for Kenyan Courts of Laws

COMPONENT	DESCRIPTION
	<p>Tools (H/w, S/w) used Tested and legally accepted Proper documentation Latest technology Accessibility Acceptability Security CIA information</p>
k k	<p>1 Forensics training and awareness-on new technologies (tools, processes, governance. Processes-recovery, analysis, examination, presentation</p>
	<p>Information security governance-security CIA of information. On how to be forensically ready. Operation governance -on how to manage DFI. IT governance-CO BIT.</p>
ikivU	<p>DFI activities; Procedures to be followed; Be scientifically sound to maintain integrity of evidence; Clear processes to stand legal scrutiny.</p>
	<p>DF team; Implements technology, processes, policies, Document processes, acquire tools Be competent team-investigators, examiners etc</p>
K! 'w'•	<p>Policies, Guideline, Procedures, Laws, Ethics On establishing and operation of DF labs Guiding staff On DF processes On CIA of information On training Legal requirements for evidence to stand to legal scrutiny On ethics of employees not to disrupt businesses Acceptance of e-evidence in court Impact of evidence act 2007.criminal procedure act 2008,communication bill 2008 be part of regulation</p>
! 'ivUi. 'l	<p>Auditing of the DF services is critical to admissibility of DF evidence presented before a court of law. Periodically audit DF processes, standards and technologies.</p>
	<p>DFI models</p>
	<p>Be authentic, complete, accurate, reliable, credible, relevant admissible</p>
• H j ; - . -	<p>The DF awareness on these dimensions is expected to unlock the potential of DF in Kenya</p>

Table 6.1: Summary of Dimensions of Validated Framework

6.3.2 Framework Validation Using Regression Analysis

When a regression analysis is run, two values of importance are the Beta Coefficient (P) and the Sig. Value (S). When a variance exhibits a high Beta value, then it implies that there is a strong unique contribution to explaining the dependent variable, when the variance explained by all other variables is explained for. The Sig. Value tells whether the variable is making a statistical significant unique contribution to the equation. If the Sig. Value is less than 0.05, then the variable is making a significant unique contribution to the prediction of the dependent variable. If the value is greater than 0.05, then you can conclude the variable is not making a significant contribution to the prediction of your dependent variable. Based on the above discussion, the proposed research model is presented below. The model summary was acceptable giving an R² value of 0.772 which is higher than 0.5.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.879(a)	.772	.746	.37892

Table 6. 3: Model Summary for Validation

The Table 6-3 shows a summary of the elements that contribute significantly towards the admissibility of digital forensics evidence services.

c		Un-standardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	8.158	.518	9.564	15.748	.000
	Technology	.450	.060	.677	7.534	.000
	People	.335	.056	.745	.629	.002
	Regulation	.469	.041	.612	1.693	.040
	Training	.478	.040	.986	-4.461	.000
	Processes	.335	.049	.617	-4.834	.000
	Governance	.262	.139	.857	.444	.000

Table 6.4: Significance and Beta Coefficients for Validation

6.3.3 Framework Validation Using AMOS

A detailed analysis on validating the framework using AMOS is given in appendix D.

CHAPTER SEVEN

CONCLUSIONS AND RECOMMENDATIONS

7.1 Achievements

The primary objective of the study was to develop a Digital Forensics Framework for Kenyan Courts of laws that will enhance growth in DF by producing forensically sound evidence before a court of law for legal proceedings.

The study was also expected to achieve the following secondary objectives;

1. Investigate the state of existing technologies, regulatory policies and legal frameworks regarding Digital Forensics in key government and private agencies involved in DF services in Kenya.
2. Investigate which factors contribute towards reliability, admissibility and authenticity of Digital Forensics.
3. Test validity of the proposed framework

We conclude by highlighting the achievement of each objective based on our research findings.

7.1.1 The Digital Forensics Framework

In the literature review, various frameworks used in the implementation of DF were discussed. A number from the developed world were cited and observation made that they heavily relied on investigative processes as the backbone of the framework. In terms of technologies, policies, training and governance, it was argued that it was not applicable in developing country like Kenya where infrastructure is poor and the cost of acquiring some of the recommended technology and training is prohibitive. This was therefore cited as a gap that needed to be filled. The legal dimension was said to be a component of building policies and procedure. As much as we agreed with the view, a weakness was found in isolating training/education and governance from the technology dimension. None of these frameworks therefore would be applied in Kenya.

A new framework was formulated comprising of six dimensions namely: Technology, Legal, Policies, Governance, training/education and processes. Technology, Legal and Governance play a major role in determining policies/procedures, training and processes. Lack of audit in various aspects of DF was noted to be prevalent. This was added to the framework. Figure 6.1 gives a diagrammatic representation of the framework.

This framework would deal effectively with known challenges of DF services in the field.

7.1.2 Digital Forensics Technologies, Policies and Legal framework

This secondary objective was achieved by investigating the level of existing technologies, regulatory policies (with respect to processes, governance, training and staff) and existing legal frameworks on DFs in key government and private agencies. Through questionnaire and interview, data was collected from CID, KACC, HIGH COURT and PWC. Of the 80 responses received 60% agree that no modern and well equipped labs existing meaning technologically we are ill prepared to handle DF services, 70 % admits that we lack trained and qualified staff to handle DF, 75% admit that we lack training and awareness to our staff on DF issues, 50% are for the opinion that current legal framework addresses DF issues, and 75 % agrees that adoption and proliferation of DF services depends on governance which we lack. These findings indicate that DF adoption in Kenya has not fully matured despite that digital crime is increasing day by day.

7.1.3 Factors Contributing to Reliability, Admissibility and Authenticity of Digital Forensics

In order to achieve this objective, we conducted a survey on technologies, regulatory policies (with respect to processes, governance, training and staff) and existing legal frameworks on DFs in key government and private agencies through interview and questionnaire. The findings indicates that of the 80 responses received, 80% agrees that proper technology means reliability of DF services, 80% are for the opinion that training and DF awareness are key to DF services, 80 % consider that proper legal frameworks contributes to proper DF services and 75% consider that governance and processes are key to adoption, proliferation and maturity of DF services.

The findings also indicate that 75% of the respondents agree that the quality of staff is key to DF. Chapter five gives detailed findings from our research.

7.1.4 Validating the Framework

The purpose of going out to collect data was to test the reliability and validity of our framework. In chapter 5, we have provided information obtained from our survey that necessitated us to introduce audit and training awareness dimensions in our Framework. These construct had different regression weights thus affects the DF services in Kenya at varying proportions.

7.2 Recommendations

It is evident from the research findings that there is need to provide a framework that will be used as a blueprint to standardize, authenticate and validate DF services in order improve chances of admissibility of e-evidence in Kenyan courts of laws. Findings and analysis discussed in chapter five clearly indicates that there is need for:-

1. Digital Forensics readiness to the current legal systems to address the shortcomings;
2. Restructuring of relevant processes to be forensically sound;
3. Digital forensic laboratories must be strengthened with skilled manpower and latest equipments and software to handle all forms of e- evidence
4. The public prosecutors must be trained to present e-evidences in a sound manner.
5. DF staff should be trained and DF processes, policies and procedures set up to guide DF services.
6. Increase funding for training to meet the growing demand of DF.

We therefore recommend the adoption of this framework as the reference framework for Digital Forensics for Kenyan courts of laws.

7.3 Further Research

As the technology in both wired and wireless computing keeps on changing and improving, more innovative and exciting services finds their way into the market. Therefore, the use of digital devices to transact both lawful and unlawful business is an emerging and interesting area of research.

Data obtained for the study from CID, KACC, High Court and PWC was of substantial amount due to the fact that such data held by such institutions is viewed to be sensitive. Similarly, protocols involved to access all the relevant people involved in DF especially in CID is involving which require a lot of time and resources. This may have introduced some bias and errors in our research findings. We therefore recommend for more thorough research in order to explore further DF issues.

7.4 Limitations of the Study

Trouble in finding necessary data-due to the nature of research, it was very hard and time consuming to convince the relevant agencies like CID/KACC that the research is purely academic and the confidentiality of their data will be guaranteed Digital Forensics is still young and in its tender stages-meaning research in the area is still scanty

APPENDIX A: REFERENCES

- Ayers, R. & Jansen, W. (2007). Guidelines on PDA Forensics. from <http://www.csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf>. Accessed on May 19, 2010.
- Becker, J., Kugler, M., and Rosemann, M., Process Management. A Guide for the Design of Business Processes, Springer: Berlin, 2003.
- Beebe N and J. G. Clark, (2004). A hierarchical Objectives-Based Framework for the Digital Investigations Process. Digital Investigation. Vol 2, pp. 147-167.
- Biros and Waiser (2006). "The Enhanced Digital Investigation Process Model", Asian Journal of Information Technology, pp. 120-150.
- Chin, W. W. (1998) "The Partial Least Squares Approach for Structural Equation Modeling," Lawrence Erlbaum Associates, pp. 295-336.
- Ciardhuain, S. O. (2004). "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, Vol 3, Issue1, 2004 from <http://wavyw.utica.edu/academic/institutes/ecii/iide/articles.cfm?action=issue&id=9>. Accessed on September 2010.
- Clark, P. (2006). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (2nd ed.). London: Elsevier Academic Press, <http://tor.eff.org/index.htmlen>.
- Cohen, J. W. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd edition). Hillsdale, NJ: Lawrence Erlbaum Associates.
- DFRWS (2001). Report from the First Digital Forensic Research Workshop. DTR-T001-01 FINAL A Road Map for Digital Forensic Research, <http://www.dfrws.org>, Accessed on August 2010.

Doran, P. (2008). Arriving at an Anti-Forensics Consensus: Examining How to Define and Control the Anti-Forensics Problem. Proceedings of the 2008 Digital Forensics Research Workshop. <http://dfrws.org/2006/proceedings/6-Harris.pdf>. Accessed on 11th May 2010.

Fornell, C. and D. Larcker (1981), .Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, Journal of Marketing Research, 28 (Feb), pp. 39-50.

Gordon, L. A.(2006) CSI/FBI Computer Crime and Security Survey, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf, Accessed on 5th February, 2010

Internet World Stats, World Internet Usage and Population Statistics News (2009). <http://www.internetworldstats.com/stats.htm> retrieved on February 2010.

Kenneally, E. (2002). Gate keeping out of the box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence. Virginia Journal of Law and Technology. Vol 6, Issue 3, Fall 2001, <http://www.violt.net/vol6/issue3/v6i3-a13-Kenneallyv.html> Accessed on 29/3/2010

Kombo, D. (2006). Proposal and Thesis Writing: An Introduction. Paulines, Publisher Africa Kenya.

Kothari, C. R. (2004). Research Methodology: Methods and Techniques. 2nd Ed, New Delhi, India: New Age International Publishers.

Losavio M, Adams J. (2006) Gap Analysis: Judicial Experience and Perception of Electronic Evidence. Journal of Digital Forensic Practice 2006; 1:13-7.

Louwrens B, Von Solms Sh, Reeckie C, Grobler T, (2006). A Control Framework for Digital Forensics, Proceedings IFIP W11.9.

Mani, S. (2006). Network Management: Principles and Practice, Dorling Kindersley, New Delhi.

McCumber, P.(2005). Dimensions of Integrated DFin Information Assurance, New Delhi, India: New Age International Publishers.

McMillian, J. (2000). Importance of a Standard Methodology in Computer Forensics. Accessed on 19 April 2010 from: <http://www.moreilly.com>

Mugenda & Mugenda (2003). Research Methods: Quantitative and Qualitative Approaches. African Centre for Technology Studies (ACTS) Nairobi, Kenya.

Rawlingson, R 2004, 'A ten step Process for Forensic Readiness', International Journal of Digital Evidence, vol. 2, no. 3.

Reith M, Varr V, Gunch G. (2002), "An Examination of Digital Forensic Models", International Journal of Digital Evidence Volume 1, Issue 3, http://www.iide.org/docs/02_art2.pdf. Accessed on 15th June 2010.

Saks, M. Koehler, J.(2005). The Coming Paradigm Shift in Forensic Identification Science. Science Magazine, 309, 892-895.

Schwartz, M. (2004). Best Practices: Collecting Computer Forensic. Retrieved 19 November 2010 from: <http://esj.com/security>.

Sommer et al. (2008). A Road Map for Digital Forensics Research. Digital Forensic Research Workshop (DFRWS) Technical Report (DTR) TOOI-01 Final.<http://www.dfrws.org/2001/dfrws-rrn-final.pdf>. Retrieved 11th march, 2010.

Sommer et al. (2007), "A Road Map for Digital Forensic Research Technical Report Technical Report DTR-T001-01", Report from the First Digital Forensic Research Workshop (DFRWS), 2007, <http://www.dfrws.org/2001/dfrws-nTi-final.ndf>, Accessed on 11th March, 2010.

Sommer (2005). Digital Evidence: Challenging the Presumption of Reliability. Journal of Digital Forensic Practice, Vol., pp 19-26.

Sommer, P. (2002). Digital evidence: Emerging Problems in Forensic Computing. International Journal of Digital Evidence, 1(1), 1 -75.

Seamus O Ciardhuain (2004). An Extended Model of Cybercrime Investigation. Journal of Digital Evidence Summer 2004; Volume 3, Issue 1.

Theodore, S (2005), Wireless Communications-Principles and Practice 2nd Ed, New Delhi: Prentice-Hall.

Von Solms, SH. and Lourens, CP (2005).A Control Framework for Digital Forensics, IFIP 11.9, **2006.**

Yin R.K (2003). Case Study Research Design and Methods, 3rd Edition, Thousands Oaks.Sage publication, inc

Werts, C., Linn, R. L. and Joreskog, K. G. (1974), "Interclass reliability estimates: testing structuralassumptions", Educational and Psychological Measurement, Vol. 34, No. 1, pp. 25-33

Websites; All accessed between Feb 2010 and Nov 2010

<http://www.cck.go.ke>

<http://www.ncirs.gov/pdffiles1/nii/199408.pdf>

<http://www.enfsi.org/ewg/fitwg/documents/>

<http://www.oip.usdoj.gov/nij/pubs-suin/>

<http://www.ncjrs.gov/pdffiles1/nij/199408.pdf>

<http://dx.doi.org/10.1080/15567280701418049>

<http://www.nhtcu.Org/ACPQ%20Guide%20v3.0.pdf>

<http://www.ncirs.org/pdffiles1/nij/199408.pdf>

http://www.dfrws.org/drrws2002/papers/Papers/Brian_carrier.pdf

<http://www.computer.org/computer/homepage/Januarv/TechNews/tcchnews2.htm>

<http://supct.law.cornell.edu/supct/litml/92-102.ZS.html>

<http://michaelnHirungi.blogspot.com>

<http://www.vjolt.net/vol6/issuc3/v6i3-a13-Kcneally.html>

<http://www.ncirs.gov/pdffiles1/nii/199408.pdf>

<http://www.enfsi.org/ewg/fitwg/documents/>

<http://www.oip.usdoj.gov/nii>

<http://www.digitalriver.com/v2.0-images/operations/naicvigi/site/media/pdf/FBIccs2005.pdf>

<http://www.iaac.orp.uk/Portals/0/Evidence9^20of%20Cyber-Crime^20v12-rev.pdf>

www.ijde.org

www.sciencedirect.com

Evidence Act Cap (80) Section 64 and 83 of 2007(Kenya).

Penal Code Act 2007(Kenya).

Criminal Procedures Act 2007(Kenya)

Communication Bill Act 2007(Kenya).

5. The technology we use comply with legal requirements



Training/Education

To what extent do you agree with the following statements regarding training in your institution conducting DF services /processes

- | | Strongly Agree | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Least Agree |
|---|----------------|---|---|---|---|---|---|---|-------------|
| 1. We have trained and qualified staff and up-to-date as a legal requirement in DF..... | n | n | n | n | n | n | n | n | n |
| 2. Training is an essential component of DF..... | . | . | . | . | . | . | . | . | . |
| 3. We undergo training and awareness regularly on DF services/processes | | | | | | | | | |
| 4. We get management and Financial support for training..... | . | . | . | . | . | . | . | . | . |
| 5. We train staff on new technologies, tools & policies regularly..... | . | . | . | . | . | . | . | . | . |

Policy and Legal issues

To what extent do you agree with the following statements regarding Policies and Legal issues with regard to Digital forensic services/processes

- | | Strongly Agree | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Least Agree |
|--|----------------|---|---|---|---|---|---|---|-------------|
| 1. We have well developed Legal and ethical, policies & procedures regarding DF.... | . | . | . | . | . | . | . | . | . |
| 2. The current laws/policies adequately address DF legal issues..... | . | . | . | . | . | . | . | . | . |
| 3. The current legal framework on DF meets the required standards of admissibility... | . | . | . | . | . | . | . | . | . |
| 4. We have a well define strategy for adopting DF tools and technologies..... | . | . | . | . | . | . | . | . | . |
| 5. We have a proper legal framework on DF that ensures admissibility of evidence.... | . | . | . | . | . | . | . | . | . |
| 6. CCK directive on SIM card registration will improve DF services..... | . | . | . | . | . | . | . | . | . |
| 7. We Collect, preserve, examine and analyses d-evidence in a forensic legal way..... | . | . | . | . | . | . | . | . | . |
| 8. We have clear guidelines on ethical behavior and code of conduct..... | . | . | . | . | . | . | . | . | . |
| 9. In your own opinion what has not yet been addressed adequately by current legal framework on DF | | | | | | | | | |

Governance

To what extent do you agree with the following statements regarding **Governance** in relation to DF services.

- | | Strongly Agree | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Least Agree |
|---|----------------|---|---|---|---|---|---|---|-------------|
| 1. The adoption, proliferation and maturation of DF depend on governance..... | . | . | . | . | . | . | . | . | . |

- 2. Our governance on DF adds value and improves the security of organization ● ● ● ● ● ● ● ●
- 3. We have in place good information security governance on DF.
- 4. In you own words, what do you think of governance in your institution?

Processes (procedure and guidelines)

To what extent do you agree with the following statements regarding DF processes available?

	Strongly Agree	7	6	5	4	3	2	1	Least Agree
1. Our procedures are scientifically sound for integrity of DF services	•								
2. We have procedures and guidelines that support our policies on DF.....	•								
3. We've defined procedures complying with industry practice, organizational practice and appropriate laws.....	•								
4. We follow procedures & practices on DF to avoid inadmissibility of evidence.....	•								
5. Proper digital forensics process guarantees admissibility of evidence.....	•								

From your experience what are the challenges facing digital forensics in Kenya.

In your own words, suggest what needs to be done to improve digital forensics processes to make the evidence more reliable, admissible, credible, complete, authentic and accurate.

- 1.
- 2.
- 3.

**SURVEY QUESTIONNAIRE FOR GOVERNMENT/PRIVATE AGENCIES
APPLYING DIGITAL EVIDENCE FROM DIGITAL FORENSICS SERVICES-
KENYAN COURTS OF LAWS**

HH MM Time interview started 1 1 1 1 1 1 DD MM YY Date of interview •• H 3 ••	HH MM Time interview ended m CD
N/B: Fill in your answers to all questions in the space provided Do not indicate your name on the questionnaire It is important that all the sections have a response	

INSTRUCTIONS

1. You are going to give your opinions based on a seven point scale, where 7 mean you **strongly agree** and 1 means **least agree** with a given statement.
2. All questions should have **ONE** answer.
3. Make sure that you tick within the box.
4. For questions where there are no numbers to be ticked, we ask you to write your answer in your own words in the space provided
5. Feel free to use additional pages, if necessary

DEMOGRAPHIC DETAILS (Important- For analysis only)

- | | | |
|--|--|---|
| Gender | Age | |
| <ul style="list-style-type: none"> • Male • Female | <ul style="list-style-type: none"> • Below 30 • 51-70 | <ul style="list-style-type: none"> • 31-50 • Above 70 |
| Education level | Income (Kshs) per month | Years served of experience |
| <ul style="list-style-type: none"> • Secondary School • College • University | <ul style="list-style-type: none"> • Less than 20,000 • 21,000 - 50,000 • More than 50,000 | <ul style="list-style-type: none"> • 2 Years and below • 3-5 Years • 6-10 Years • Above 10Years |
| Level of court currently presiding | Years in your current position | Approximate no of years of DF experience |
| <ul style="list-style-type: none"> • 2 Years and below • 3-5 Years • 6-8 Years • Above 8 Years | <ul style="list-style-type: none"> • 2 Years and below • 3-5 Years • 6-8 Years • Above 8 Years | <ul style="list-style-type: none"> • 2 Years and below • 3-5 Years • 6-8 Years • Above 8 Years |

- Q1. Has any party offered digital forensic evidence (or evidence from the computer forensics process) in any evidentiary motion or trial over which you have presided?
- YES • NO
- Q2. What issues, if any, have you faced in deciding on how to rule on challenges to the admissibility of digital forensics;
- Q3. Will you require lawyers to meet a higher standard than for physical forensic evidence when they seek to authenticate and admit digital forensic evidence? For example, will you require a higher standard when they seek to authenticate and admit evidence retrieved from business records databases, e-mail, or Web sites?
- YES • NO

Q3A. If "yes" to Q3, what are the concerns that prompt you to require this higher standard and/or what is the informational basis that catalyzed this higher standard?

Q3B. If "yes" to Q3, what specific facts and circumstances must the lawyer establish in order to satisfy your concerns?

Q5. What factors lead to a more (or less) effective presentation of digital evidence to a fact-finder?

Q7. On a scale of 1 to 7 (with 1 being the lowest and 7 being the highest), how would you rate your own familiarity with:

Q7A. Digital forensic evidence 7 6 5 4 3 2 1
• • • • • • •

Q7B. The digital forensics process P . _ _ _ _ _

Q7C. Digital forensics technologies O O D O n D C

Q7D. Digital forensics policies and laws O O D O n D C

Q8. What factors have influenced your ratings in Question 7 (e.g., education, personal experience, professional training, etc.)?

Q9. Do you believe that you have more, the same, or less understanding of digital forensic evidence compared to your peer judges:

Q9A. Locally? • MORE • SAME • LESS

Q9B. Nationally? • MORE • SAME • LESS

Q10. How does the technical understanding of the prosecutors presenting digital evidence at hearings and at trial affect the effectiveness of that evidence to the fact-finder?

Technology

To what extent do you agree with the following statements regarding technology with respect to Digital Forensics in Kenyan

- | | Strongly Agree | Least Agree |
|---|----------------|-------------------|
| | 7 6 5 4 3 2 1 | 7 6 5 4 3 2 1 |
| 1. We have proper technology in place for DF processes/services | • • • • • • • | • • • • • • • |
| 2. Poor technology in place compromises admissibility of D-evidence..... | • • • • • • • | • • • • • • • ! ! |
| 5. The technology we use is reliable, precise, accurate, non-reputable, secure, flexible, and inexpensive | • • • • • • • | • • • • • • • |

Legal and ethics

To what extent do you agree with the following statements regarding legal and ethical issues

- | | Strongly Agree | Least Agree |
|---|----------------|---------------|
| | 7 6 5 4 3 2 1 | 7 6 5 4 3 2 1 |
| 1. The legal and ethical in place adequately address DF services..... | • • • • • • • | • • • • • • • |
| 4. Reliability of digital evidence in court depends on legal systems..... | • • • • • • • | • • • • • • • |
| 5. Credibility of D-evidence is dependent on proper legal structures..... | • • • • • • • | • • • • • • • |

Regulations (policies, procedures, practices, standards)

To what extent do you agree with the following statements regarding **Regulations** on the Digital forensics services in Kenyan courts of laws

Strongly Least
Agree Agree
7 6 5 4 3 2 1

- 1. We have proper policies, practices, procedures and standards on
- 2. Proper regulations on DF enhance admissibility of e-evidence. n n n n r i n n

Training/Education

To what extent do you agree with the following statements regarding training of staff on DF processes

Strongly Least
Agree Agree
7 6 5 4 3 2 1

- 1. We undergo training and awareness on DF regularly. • • • • • [!
- 2. We have trained and qualified staff on DF services/processes. • • • • • [!
- 3. Training /educations is a major key to DF successes. • • • • •
- 4. The quality of staff determines growth and maturity of DF services. • • • • •

Governance

To what extent do you agree with the following statements regarding governance on DF processes

Strongly Least
Agree Agree
7 6 5 4 3 2 1

- 1. There is adequate governance on DF services. • • • • •
- 2. Good governance on DF ensures reliability of e-evidence. • • • • •
- 3. Governance is a key component on DF services/processes. • • • • •
- 4. Good governance on DF ensures admissibility of e-evidence. • • • • •

Processes

To what extent do you agree with the following statements regarding processes on DF

Strongly Least
Agree Agree

7 6 5 4 3 2 1

- 1. We have proper processes in place for DF services for sound evidence. • • • • •
- 2. Processes should be a major element of DF services. • • • • •

APPENDIX C: QUESTIONNAIRE ITEMS

Table CI. QUESTIONNAIRE ITEMS

VARIABLE	ITEM	
Technology	T1	Availability =usage of tested/acceptable legally
	T2	Affordability
	T3	Acceptability
	T4	Security -CIA
	T5	Adaptability
	T6	Comprehensive tech
Legal and Ethical (Regulation)	LE1	Available
	LE2	Applied
	LE3	Suitability
	LE4	Implies good technology
	LE5	Implies quality people
	L6	Implies processes used
	LE7	Admissibility
Governance	G1	Available.
	G2	Level
	G3	Relevant
	G4	Irrelevant
	G5	
	G6	
Training /Education	TE1	Available/essential/key
	TE2	Regular/training awareness
	TE3	Adequate /financial
	TE4	Relevant
	TE5	Affordable
People	PI	Available
	P2	Relevant
	P3	Workable
	P4	
Processes	PR1	Done
	PR2	Regular
	PR3	Relevant
	PR4	Funded
	PR5	Useful

Measure reliability was assessed using internal consistency scores, calculated by the composite reliability scores (Werts et al., 1974). Internal consistencies of all variables are considered acceptable since they exceed .70, signifying tolerable reliability, this is shown in Table C2.below.

Table C2. Composite Reliability

Construct	Composite Reliability
Technology	0.7864
Legal/Regulation	0.8159
Governance	0.7870
Training /Education	0.9243
People	0.8284
Processes	0.9457

Establishing discriminant validity requires an appropriate AVE (Average variance Extracted) analysis, we tested to see if the square root of every AVE (there is one for every latent construct) is much larger than any correlation among any pair of latent construct. As a rule of thumb, the square root of each construct should be much larger than the Correlation of the specific construct with any of the other constructs in the model (Cohen, 1998) and should be at least 0.5 (Fornell and Larcker, 1981). This is shown in Table C3,

Table C3. Average Variance Extracted

Construct	Average Variance Extracted	Square Root AVE
Technology	0.6630	0.8503
Legal/Regulation	0.7180	0.8861
Governance	0.4944	0.7280
Training /education	0.5095	0.7399
People	0.7235	0.8896
Processes	0.6015	0.8082

Table C4. Correlations of Latent Variables

	Technology	Legal	Governance	Training	People	Processes
Technology	0.7603					
Legal/regulation	0.5203	0.6976				
Governance	0.4331	0.3921	0.5442			
Training/educated	0.4980	0.4125	0.3397	0.5538		
People	0.4917	0.4108	0.3434	0.3598	0.7021	
Processes	0.4600	0.4151	0.4785	0.4467	0.5070	0.7209

APPENDIX D: MODIFICATION INDICES

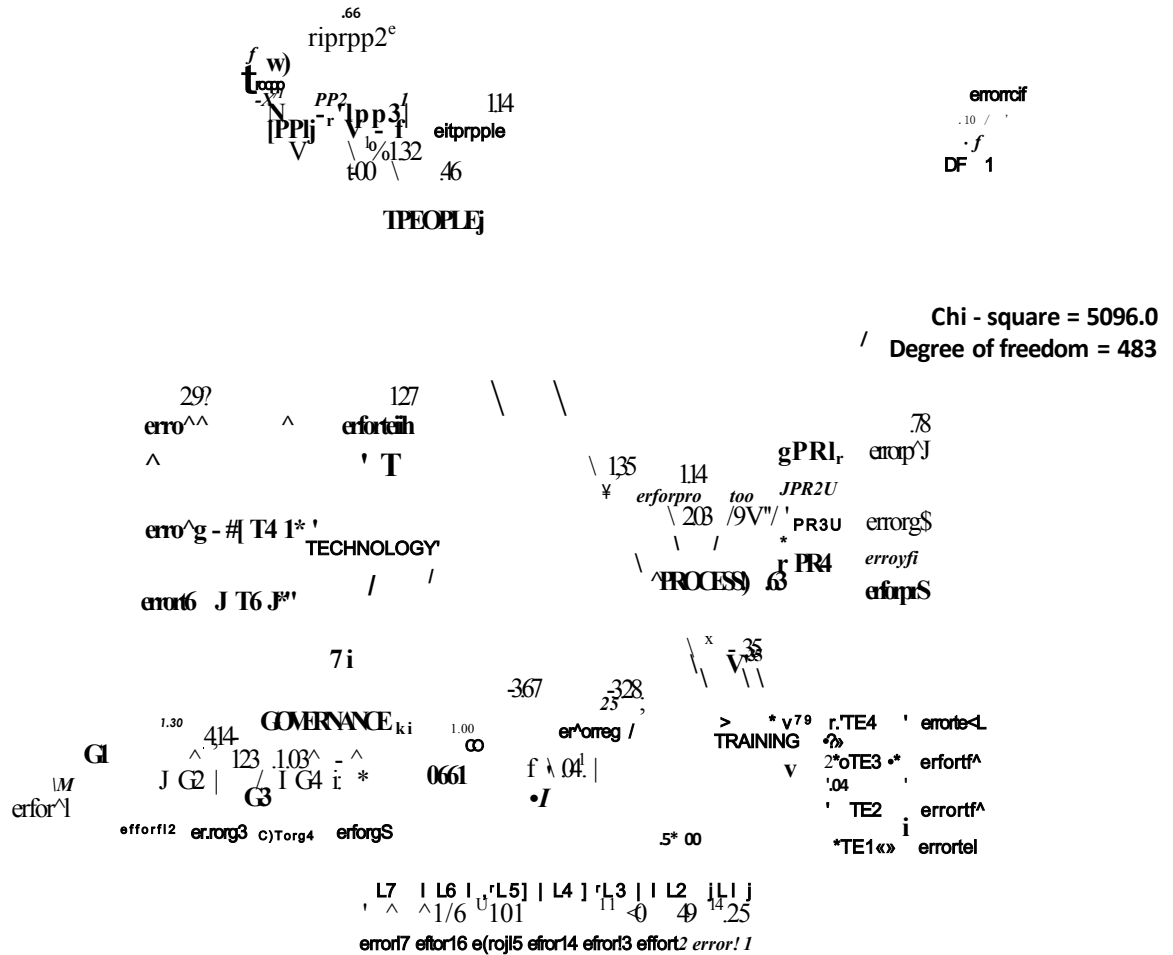


Figure DJ. Graphical Representation the Unfitted Model

Estimates (Group number 1 - Default model)

Scalar Estimates (Group number 1 - Default model)

Maximum Likelihood Estimates

Arbuckle (2005) mentions that model evaluation is one of the most difficult and unsettle issues related to structural equation modeling. In this research the model is validated using confirmatory factor analysis (CFA).The CFA is carried out using SEM software AMOS 16. The objective of the CFA is to construct a structural model which aligns the tested measures to the specific constructs, by constraining the variance of each measure to the specific latent construct it should represent. In addition to assess the degree to which each measure contributes to its latent construct, the CFA also tests the separation between constructs by evaluating the fit in the overall model. There are four groups of fit measures. The fit measures within each group give the same rank of ordering of models (Arbuckle 2005). The first group is RMSEA and TLI, the second groups is CFI, the third group is CMIN and NFI, and the fourth group is GFI, and AGFI. Among the many measures of fit, five popular measures are: Chi-square (χ^2/df), goodness of fit index (GFI), Tucker-Lewis Index (TLI) and Root Mean-Square Error of Approximation (RMSEA) (Holmes-Smith 2000). Figure above shows the initial research model before it was fit to the research data (un-standardized)

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
REGULATION	<—	GOVERNANCE	-.001	.004	-.296	.767	
REGULATION	<~	TRAINING	.008				
REGULATION	< -	errorreg	.038				
PEOPLE	<—	GOVERNANCE	.097	.119	.813	.416	
PROCESS	<—	GOVERNANCE	.798	.325	2.455	.014	
TECHNOLOGY	<—	GOVERNANCE	.437				
TECHNOLOGY	<—	REGULATION	-3.666				
PEOPLE	<—	REGULATION	2.752				
PROCESS	<—	REGULATION	-3.281				
PROCESS	<---	TRAINING	-.346				
TECHNOLOGY	<—	TRAINING	.088				
PEOPLE	< --	TRAINING	1.346				
PEOPLE	<—	errorpple	.459				
PROCESS	< -	errorpro	2.028				
TECHNOLOGY	<---	errortech	1.031				
PP1	<—	PEOPLE	1.000				
PP2	<—	PEOPLE	1.220	.288	4.243	***	
PP3	<—	PEOPLE	1.320	.318	4.147	***	
T6	<—	TECHNOLOGY	1.351				

			Estimate	S.E.	C.R.	P	Label
T5	<—	TECHNOLOGY	.923				
T4	<—	TECHNOLOGY	1.526				
T3	<—	TECHNOLOGY	1.116				
T2	<—	TECHNOLOGY	.895				
T1	<—	TECHNOLOGY	.758				
PR1	<—	PROCESS	1.000				
PR2	<—	PROCESS	.912	.069	13.219	***	
PR3	<—	PROCESS	.759	.084	9.037	***	
PR4	<—	PROCESS	.698	.086	8.132	***	
PR5	<—	PROCESS	.825	.078	10.541	***	
G7	<—	GOVERNANCE	1.000				
G6	<—	GOVERNANCE	1.092	.156	7.007	***	
G5	<—	GOVERNANCE	.953	.148	6.431	***	
G4		GOVERNANCE	1.028	.150	6.856	***	
G3	<—	GOVERNANCE	1.229	.163	7.559	***	
G2	<—	GOVERNANCE	1.136	.179	6.363	***	
G1	<—	GOVERNANCE	1.304	.185	7.033	***	
TE5	<—	TRAINING	1.505				
TE4	<—	TRAINING	.795				
TE3	<—	TRAINING	.281				
TE2	<—	TRAINING	2.202				
TE1	<—	TRAINING	2.035				
LI	<—	REGULATION	1.000				
L2	<—	REGULATION	24.515				
L3	<—	REGULATION	36.988				
L4	<—	REGULATION	16.084				
L5	<—	REGULATION	3.057				
L6	<—	REGULATION	23.068				
L7	<—	REGULATION	-.672				
DF	<—	PEOPLE	.049				
DF	<—	TECHNOLOGY	.100				
DF	<—	PROCESS	.041				
DF	<—	errorrdf	.100				

Model Fit Summary

CMIN: CMIN/DF<3, THEN MODEL IS FIT

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	89	953.846	483	.000	1.975
Saturated model	561	.000	0		
Independence model	33	1948.555	528	.000	3.690

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.552	.610	.547	.525
Saturated model	.000	1.000		
Independence model	.976	.299	.255	.282

Baseline Comparisons:

Model	NFI Delta 1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.510	.465	.679	.638	.669
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Parsimony-Adjusted Measures

Model	PRATIO	PNFI	PCFI
Default model	.915	.467	.612
Saturated model	.000	.000	.000
Independence model	1.000	.000	.000

NCP

Model	NCP	LO 90	HI 90
Default model	470.846	386.902	562.568
Saturated model	.000	.000	.000
Independence model	1420.555	1289.260	1559.384

FMIN

Model	FMIN	FO	LO 90	HI 90
Default model	12.074	5.960	4.897	7.121
Saturated model	.000	.000	.000	.000
Independence model	24.665	17.982	16.320	19.739

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.111	.101	.121	.000
Independence model	.185	.176	.193	.000

AIC

Model	AIC	BCC	BIC	CAIC
Default model	1131.846	1266.334	1343.846	1432.846
Saturated model	1122.000	1969.733	2458.317	3019.317
Independence model	2014.555	2064.421	2093.162	2126.162

ECVI

Model	ECVI	LO 90	HI 90	MECVI
Default model	14.327	13.265	15.488	16.030
Saturated model	14.203	14.203	14.203	24.933
Independence model	25.501	23.839	27.258	26.132

HOELTER

Model	HOELTER	HOELTER
	.05	.01
Default model	45	47
Independence model	24	25

SUMMARY OF ABOVE BEFORE

Fit Measures	Standards Fit	Model Fit
X2/DF	A value close to 1 and not exceeding 3 indicates a good fit	1.975
IFI	IFI values close to 1 indicate a very good fit.	0.679
TLI	A value close to 1 indicates a very good fit	0.978
NFI	Values close to 1 indicate a very	0.510

	good fit	
CFI	a value close to 1 indicates a very good fit	0.669
RFI	RFI values close to 1 indicate a very good fit	0.798
RMSEA	A value should not greater than 0.1	0.111

AFTER CHANGE:

Fit Measures	Standards Fit	Model Fit
X2/DF	A value close to 1 and not exceeding 3 indicates a good fit	1.975
IFI	IFI values close to 1 indicate a very good fit	0.879
TLI	a value close to 1 indicates a very good fit	0.978
NFI	values close to 1 indicate a very good fit	0.710
CFI	a value close to 1 indicates a very good fit	0.869
RFI	RFI values close to 1 indicate a very good fit	0.798
RMSEA	A value should not greater than 0.1	0.011

The following graphic represents the result of testing the structural links of the research model using Analysis of Moment Structures (AMOS 16). The estimated path coefficients are given along with the standardized regression weights. Structural equation modeling is well suited to test a group of constructs simultaneously in the form of a model with significant level 0.05. It helps to reveal these hypotheses and to consider each one individually.

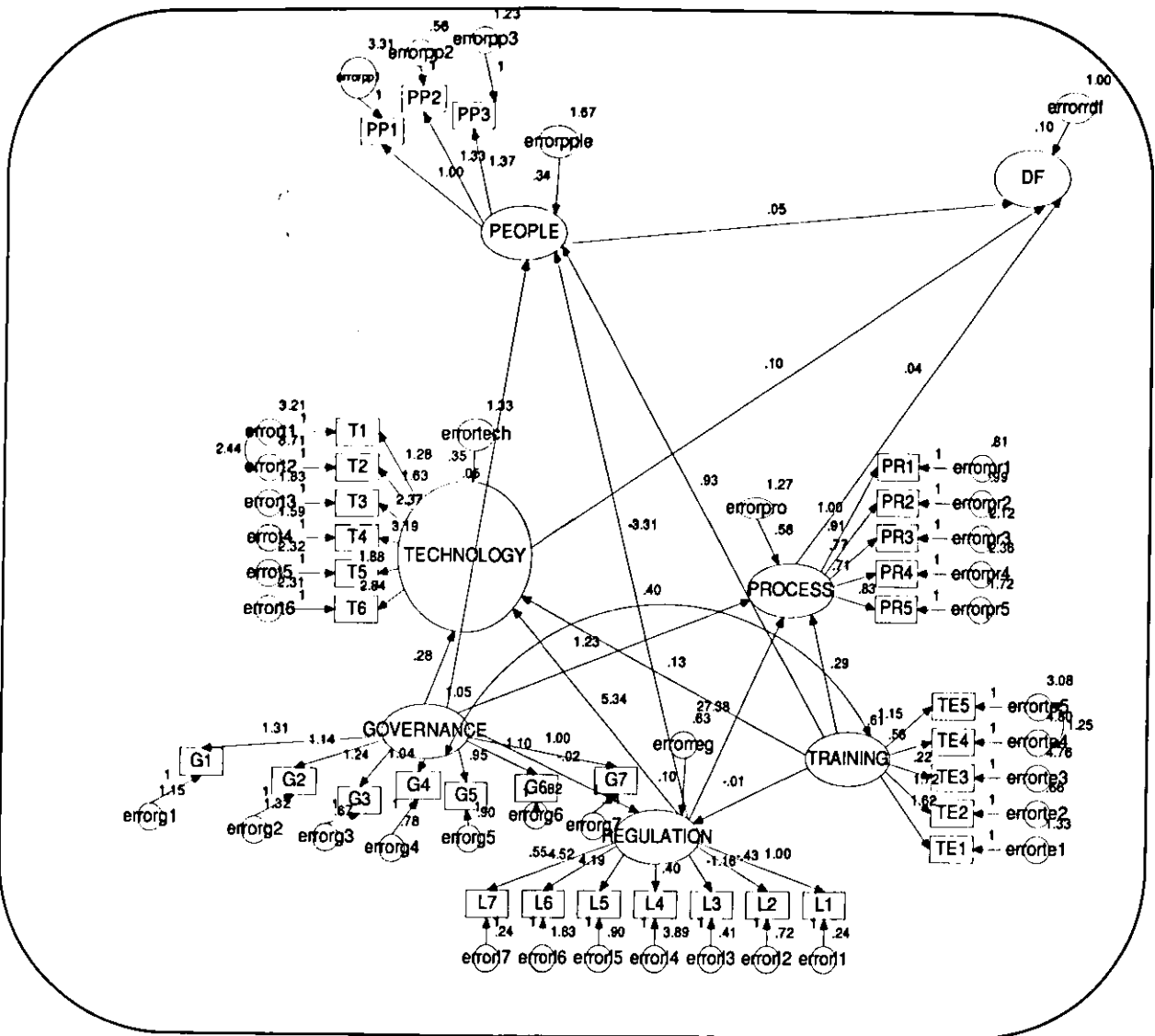


Fig. D1: Modification Indices (Group number 1 - Default Model)

Covariances: (Group number 1 - Default model)

		M.I.	Par Change
errorpro	<--> errortech	27.867	.820
errorte4	<--> errorte3	13.901	2.004
errorteS	<--> errorte3	21.837	2.046
errorg2	<--> errorg1	44.391	1.024
errorg7	<--> errorg6	19.118	.455
errorpr5	<--> errorg2	12.236	-.660
errort2	<--> errort1	40.218	2.375

Variances: (Group number 1 - Default model)

M.I. Par Change

Regression Weights: (Group number 1 - Default model)

		M.I.	Par Change
PROCESS	<— errortech	27.867	1.314
PROCESS	TECHNOLOGY	22.914	1.048
TECHNOLOGY	<— errorpro	27.867	.743
TECHNOLOGY	<— PROCESS	24.485	.322
TE3	TE4	13.154	.399
TE3	TE5	16.443	.505
TE4	<— TE3	13.804	.418
TE5	TE3	21.685	.426
G1	<— G2	20.152	.354
G2	<— G1	15.175	.307
T1	T2	27.901	.480
T2	<— T1	29.374	.594

Table D1 Modification Indices (Group number 1 - Default model)

Covariances: (Group number 1 - Default model)

		M.I.	Par Change
errorl2	<--> errorl3	31.396	.343
errorte4	<--> errorte3	13.542	1.965
errorte5	<--> errorte3	20.943	1.984
errorg2	<--> errorg1	44.562	1.033
errorg7	<--> errorg6	19.401	.460
errorpr5	<--> errorg2	12.424	-.666

Variances: (Group number 1 - Default model)

M.I. Par Change

Regression Weights: (Group number 1 - Default model)

	M.I.	Par Change
L3 <--- L2	31.266	.478
L2 <--- L3	30.398	.806
TE3 <-- TE4	12.676	.391
TE3 <--- TE5	15.412	.488
TE4 <--- TE3	13.359	.409
TE5 <~ TE3	20.661	.413
G1 <--- G2	20.412	.358
G2 <--- G1	15.417	.310
PP1 <--- PROCESS	11.628	.322
PP1 <--- PR3	11.687	.313
PP1 <--- PR1	10.785	.280

Table D2: Modification Indices (Group number 1 - Default model)

Covariance's: (Group number 1 - Default model)

	M.I.	Par Change
errorl2 <--> errorl3	31.375	.343
errorte5 <--> errorte3	14.603	1.520
errorg2 <--> errorgl	44.550	1.032
errorg7 <--> errorg6	19.404	.460
errorpr5 <--> errorg2	12.446	-.667

Variances: (Group number 1 - Default model)

M.I. Par Change

Regression Weights: (Group number 1 - Default model)

	M.I.	Par Change
L3 <--- L2	31.230	.477
L2 <--- L3	30.346	.805
TE3 <--- TE5	11.012	.375
TE5 <--- TE3	21.558	.425
G1 <--- G2	20.394	.358
G2 <--- G1	15.402	.310

	M.I.	Par Change
PPI <--- PROCESS	11.576	.321
PPI <--- PR3	11.672	.313
PPI <--- PR1	10.701	.279

Table D3: Modification Indices (Group number 1 - Default model)

Covariances: (Group number 1 - Default model)

	M.I.	Par Change
errorpro <--> errortech	27.264	.824
errorte5 <--> errorte3	14.908	1.545
errorg7 <-> errorg6	14.188	.359

Variances: (Group number 1 - Default model)

M.I. Par Change

Regression Weights: (Group number 1 - Default model)

	M.I.	Par Change
PROCESS <--- errortech	27.264	1.302
PROCESS <--- TECHNOLOGY	23.188	1.048
TECHNOLOGY <--- errorpro	27.264	.709
TECHNOLOGY <-- PROCESS	23.399	.315
TE3 <- TE5	11.453	.383
TE5 <--- TE3	22.228	.435

Table D4: Modification Indices (Group number 1 - Default model)

Covariances: (Group number 1 - Default model)

	M.I.	Par Change
error12 <--> error13	31.140	.339
errorte5 <--> errorte3	14.621	1.520
errorg7 <--> errorg6	14.875	.372
errorpp3 <--> errorg7	10.501	-.410

Variances: (Group number 1 - Default model)

M.I. Par Change

Regression Weights: (Group number 1 - Default model)

	M.I.	Par Change
L3 ← L2	30.767	.471
L2 ← L3	29.580	.793
TE3 TE5	11.016	.376
TE5 ← TE3	21.540	.425
PP1 ← PROCESS	11.417	.321
PP1 PR3	11.522	.312
PP1 ← PR1	10.592	.278

Table D5: Modification Indices (Group number 1 - Default model)

Covariances: (Group number 1 • Default model)

	M.I.	Par Change
errorte5 <--> errorte3	14.479	1.514
errorg7 <--> errorg6	15.011	.374
errorpp3 <--> errorg7	10.920	-.424

Variances: (Group number 1 - Default model)

M.I. Par Change

Regression Weights: (Group number 1 - Default model)

	M.I.	Par Change
TE3 ← TE5	10.921	.374
TE5 ← TE3	21.443	.424
PP1 ← PROCESS	11.661	.323
PP1 ← PR3	11.779	.314
PP1 <--- PR1	10.904	.281

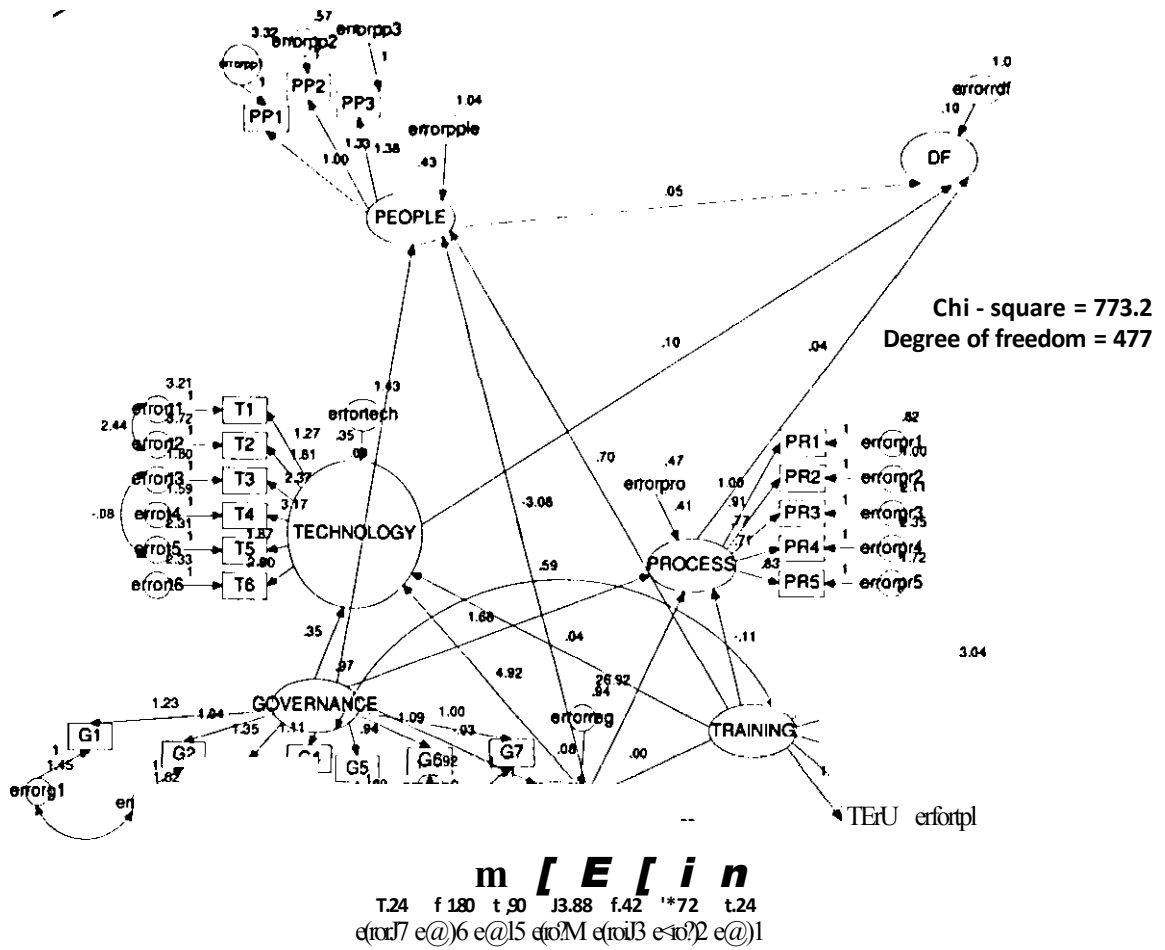


Fig. D2. The Standardized DF Model for Kenyan Courts of Laws.