

ADOPTABILITY MODEL FOR DIGITAL FORENSIC EVIDENCE IN KENYA

CHEPKWONY JOYCE CHEPKEMOI

**A Thesis submitted to the Institute of Postgraduate Studies of Kabarak University in
Partial Fulfilment of the Requirements for the Award of the Master of Science
Degree in IT Security and Audit.**

KABARAK UNIVERSITY

OCTOBER, 2018

DECLARATION

I declare that this is my original work and has never been presented for the award of a degree in any other institution, and that all references are accurately reported.

Signature:

Date:

Joyce Chepkemoi Chepkwony

Reg No.: GMIA/NE/0856/05/16

RECOMMENDATION

To the Institute of Postgraduate Studies:

The Research Proposal entitled “**Adoptability Model for Digital Forensic Evidence in Kenya**”, written by **Chepkwony Joyce Chepkemoi**, is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the Research Proposal and recommend it to be accepted in partial fulfilment of the Requirements for the Degree of Doctor of Philosophy in Counseling Psychology.

Signature:

Date:

Prof. Kefa Rabah

School of Computer Science and Bioinformatics,
Kabarak University.

Signature:

Date:

Prof. Simon M. Karume

Department of Computing and Informatics,
Laikipia University.

COPYRIGHT

© 2018

Joyce Chepkemoi Chepkwony

All the rights are reserved. No part of this thesis should be produced or transmitted in any form including photocopying, recording or retrieving from system without permission of the researcher or Kabarak University.

ACKNOWLEDGMENT

I would like to thank everyone who has contributed to the successful completion of this thesis. I express my gratitude to my research supervisors, Prof. Kefa Rabah and Prof. Simon Karume for their good suggestions and guidance throughout the development of this thesis. In addition, I would also like to express my gratitude to my loving family, especially my husband Mr. David Kemei who helped me by giving encouragement when I felt exhausted and out of options.

DEDICATION

This thesis is dedicated specifically to my beloved husband and children who have always stood by me and dealt with all my absence from many family occasions with a smile.

ABSTRACT

The traditional techniques used by forensic investigators through the incident response operations include mostly pulling out the power cable of the suspected machines. This method normally causes a major interference of the evidence gathering process, hence the need for a better investigation method. The purpose of the study was to provide a means for the Kenya Police in evaluating their forensic adoptability in digital forensic evidence. This study was intended for those who were operating in the fields of computer forensics. The main objective was to investigate the adoptability of digital forensics in digital crime handling in Kenya. The researcher came up with a better method by analysing different existing methods and techniques in the literature review that allowed an investigator to scrutinize and perform forensic acquisition in a running system without inducing the effects of taint or forensic blurriness caused by scrutinizing and analyzing a running system, and collect evidence. Descriptive research design was adopted. Data collection was done by use of questionnaires and analysed through qualitative and quantitative techniques. The target population was drawn from the Kenya Police in Nakuru County, Kenya. Stratified and purposive sampling was applied so as to get the respondents based on the representative and feasibility of attaining the necessary data. The study established that there was low level of effectiveness regarding digital forensic services necessary to improve the admissibility of evidence in court. Similarly, technology used in institutions complied with legal requirements, however little review was being done to ensure that the system they used met quality needs of their organizations. Finally, although digital forensic tools existed in the institutions, respondents felt a dire need for additional digital forensic tools. The study recommends that more trainings and awareness program must be given priority by the Kenya Police as regards digital forensic evidence acquisition and handling. Likewise, it is prudent for the Kenya Police to channel more resources towards digital evidence acquisition tools and services to improve admissibility of digital evidence in courts.

Key words: Acquisition, Admissibility, Digital, Evidence, Forensic, Investigation.

TABLE OF CONTENTS

DECLARATION.....	ii
RECOMMENDATION.....	iii
COPYRIGHT.....	iv
ACKNOWLEDGMENT.....	v
DEDICATION.....	vi
ABSTRACT.....	vii
LIST OF TABLES.....	xii
LIST OF FIGURES.....	xiii
OPERATIONAL DEFINITION OF TERMS.....	xiv
LIST OF ABBREVIATIONS AND ACRONYMS.....	xv
CHAPTER ONE.....	1
INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Background to the Study.....	1
1.3 Statement of the Problem.....	4
1.5 Objectives of the Study.....	4
1.5.1 Specific Objectives.....	5
1.6 Research Questions.....	5
1.7 Significance of the Study.....	5
1.8 Scope of the Study.....	6
1.9 Limitations of the Study.....	6
1.10 Assumptions of the Study.....	6
CHAPTER TWO.....	7
LITERATURE REVIEW.....	7
2.1 Introduction.....	7
2.2 Digital Forensic.....	7
2.3 Effectiveness of Digital Forensic in Digital Crime Handling.....	8
According to Grobler, Louwrens and Solm (2010), digital forensic is deemed effective if it has the ability to produce desired results. The performance of digital forensic tools presents different strengths and weaknesses as opposed to their declared capabilities.	8
2.3.1 Digital Crime Handling.....	8

2.3.2 Digital Forensics in Law	10
2.3.3 Effectiveness of Digital Forensic in Kenya	10
2.4 Contribution of Technology, Legal Framework and Regulatory Policies towards Admissibility of Digital Forensics	11
2.4.1 Chain of Custody	11
2.4.2 Legal Aspect	11
2.4.3 Digital Forensics Security Fundamentals	12
2.4.4 Threat Intelligence	12
2.4.5 Code of Ethics.....	12
2.4.6 Technologies Used in Forensic	13
2.4.7 Guidelines and Principles	13
2.4.7.1 ISO/IEC 27037:2012	13
2.4.7.2 Association of Chief Police Officers (ACPO).....	14
2.4.8 Approach for Creation of Cyber Laws.....	14
2.4.9 Constitutional Law.....	15
2.4.10 Challenges in Law Enforcement.....	15
2.5 Components for Forensically Sound Digital Data Acquisition	16
2.5.1 Tools and Materials for Collecting Digital Evidence	16
2.5.2 The Cyber Tools On-Line Search for Evidence (CTOSE).....	22
2.5.3 Components that May Cause Inadmissibility of Evidence	22
2.5.4 Digital Forensic Processes	23
2.5.5 Steps in Digital Evidence Acquisition	25
2.5.6 Digital Evidence Acquisition Methods.....	26
2.5.7 Digital Evidence Transportation	26
2.6 Empirical Review.....	27
2.7 Conceptual Framework.....	30
2.8 Gaps in the Literature.....	32
CHAPTER THREE	33
RESEARCH DESIGN AND METHODOLOGY	33
3.1 Introduction.....	33
3.2 Research Design.....	33
3.4 Population of the Study.....	33

3.5 Sampling procedures and Sampling size	34
3.5.1 Sampling Procedure	34
3.5.2 Sample Size.....	35
3.6 Instrumentation	35
3.7 Data Analysis	35
3.8 Model Design and Implementation.....	36
3.8.1 Model Design.....	36
3.8.2 Model Implementation.....	36
3.9 Ethical Consideration.....	36
CHAPTER FOUR.....	37
DATA ANALYSIS, PRESENTATION AND DISCUSSION	37
4.1 Introduction.....	37
4.2 Demographic Information.....	37
4.2.1 Gender.....	37
4.2.2 Highest Academic Qualification.....	37
4.2.3 A Cross tabulation of Gender and Length of Employment	38
4.2.4 Current Rank.....	38
4.2.5 Total Working Experience in the Field of Forensics	39
4.2.6 Familiarity to the Digital Forensics	39
4.3 Admissibility in Court of Law	39
4.3.1 Effectiveness of Digital Forensic in Digital Crime Handling.....	40
4.4 Technology, Legal Framework and Regulatory Policies.....	41
4.5 Components for Forensic Digital Evidence.....	42
4.6 Adoptability of Digital Forensic	43
4.7 Model Derivation	43
4.8 Regression Analysis.....	45
4.8.1. Regression Weights	46
4.9 Model Development.....	46
4.9.1 Purpose of the Model.....	46
4.9.2 System Functional Overview	46
4.9.3 Software Engineering and Design	49
4.10 Evaluation of the Model.....	63

4.11 Security of the Model.....	65
4.12 Areas of Further Improvement.....	65
CHAPTER FIVE	66
CONCLUSIONS AND RECOMMENDATIONS.....	66
5.1 Introduction.....	66
5.2 Conclusions.....	66
5.2.1 Research Question 1: How can Digital Forensics in Digital Crime Handling in Kenya Police Service be Effective?	66
5.2.2 Research Question 2: How will Technology, Legal Framework, Regulatory Policies and Practices Contribute towards Admissibility of Digital Forensics?	66
5.2.3 Research Question 3: What are the Outcomes of the Examination of the Essential Components that Make up Forensically Sound Digital Data Acquisition Process?	67
5.2.4 Research Question 4: How will the Adoptability Model be developed?	67
5.3 Recommendations.....	67
5.3.1 Training and Awareness	68
5.3.2 Recommendations for further research	68
REFERENCES.....	69
APPENDIX I: Letter of Introduction	75
APPENDIX II: Questionnaire for the Kenya Police Service	76
APPENDIX III: System Code.....	81
APPENDIX IV: Permission to carry out Academic Research	86
APPENDIX V: Research Authorization (NACOSTI)	88
APPENDIX VI: Research Permit (NACOSTI).....	89
APPENDIX VII: Research Authorization (County Commissioner).....	90
APPENDIX VIII: Research Authorization (County Director of Education).....	91
APPENDIX IX: Introduction Letter (Kabarak University).....	92

LIST OF TABLES

Table 1: Comparison of Forensic Tools Function	16
Table 2: Exploring Static and Live Digital Forensics: Methods, Practices and Tools	18
Table 3: Comparison of Traditional Forensic Versus Live Forensic	21
Table 4: A list of Digital Forensic Investigation Model.	28
Table 5: The Target Population.	34
Table 6: Gender.....	37
Table 7: Highest Academic Qualification.....	37
Table 8: Cross tabulation of Gender and Length of Employment	38
Table 9: Current Rank.....	38
Table 10: Working Experience in the Field of Forensics	39
Table 11: Familiarity to the Digital Forensics	39
Table 12: Effectiveness of Digital Forensic in Digital Crime Handling	40
Table 13: Technology, Legal Framework and Regulatory Policies	41
Table 14: Components for Forensic Digital Evidence.....	42
Table 15: Adoptability of Digital Forensic	43
Table 16: Correlation Analysis	44
Table 17: Model Summary	45
Table 18: ANOVA ^a	45
Table 19: Coefficients ^a	46
Table 20: Model Evaluation.....	64

LIST OF FIGURES

Figure 1: Information Security Management.....	12
Figure 2: CIRT-Level Response to Advanced Persistent threat	24
Figure 3: Abstract Digital Forensics Model.....	29
Figure 4: Technological Adoptability Model.	30
Figure 5: Conceptual Framework.	31
Figure 6: System Architecture	48
Figure 7: User Registration Form	50
Figure 8: Registration Flowchart	50
Figure 9: Login Flowchart	51
Figure 10: Login Form.....	52
Figure 11: Dashboard with no Active Assessments for the Logged in User	53
Figure 12: Dashboard with One Active Assessment for the Logged in User.....	53
Figure 13: Header Menu.	54
Figure 14: Footer Menu.	54
Figure 15: Forensic Assessments Page	55
Figure 16: Adoptability of Digital Forensics Flowchart.....	55
Figure 17. Forensic Adoptability Index Gauge.....	56
Figure 18: Forensic Adoptability Indicators	57
Figure 19: Model Cases	58
Figure 20: Statistics Panel.....	59
Figure 21: Forensic Score Flowchart.....	59
Figure 22. Forensic Scores in HTML Output	60
Figure 23: Forensic Scores in PDF Output	60
Figure 24: Forensic Recommendations Flowchart.	61
Figure 25: Forensic Recommendation HTML.....	61
Figure 26: Forensic Recommendation PDF.....	61
Figure 27: Forensic Help Module	62
Figure 28: Entity Relationship Diagram	63
Figure 29. User Verification – Professional Analysis	65

OPERATIONAL DEFINITION OF TERMS

A Crime Scene Investigator (CSI)	This is a member of the law enforcement who is responsible for identifying, acquiring, preserving and presenting the physical evidence at the scene of a crime (Fisher & Fisher, 2012).
Acquisition	Process of creating a copy of data within a defined set (Nikkel, 2006).
Admissibility	Any testimonial, documentary, or tangible evidence that may be introduced to a fact finder- usually a judge or jury – to establish or to bolster a point put forth by a party to the proceeding in a court of law. (Murphy & Glover, 2015)
Analysis	The process of breaking a difficult topic into smaller parts in order to achieve a better understanding of it (Beaney & Summer, 2012).
A model	This is a representation of a system or process created on a computer, to assist calculations and predictions (Card, 2017).
Collection	Process of gathering items that contain potential digital evidence (Casey, 2011).
Dead acquisition analysis	This is analysis done on a powered off computer (Jones, 2008).
Digital (photographs, video and audio)	A digital system uses discrete values rather than the continuous spectrum values of analog. It can refer to the type of data storage and transfer, the internal working of a device, or the type of display (Skoog <i>et al.</i> , 2017).
Digital evidence or electronic evidence	Is any probative information stored or transmitted in digital form that a party to a court case may use at trial (Casey, 2011).
Effectiveness	This is the ability of produce a desired result or the ability to produce desired output (Gupta, 2016).
Encryption	It is the translation of data into a secret code. Most effective way to achieve data security (Sahai & Waters 2014).
Legal Authority	It is a form of leadership in which the authority of an organization or a ruling regime is largely tied to legal rationality, legal legitimacy and bureaucracy. (Tyler & Jackson, 2014).
Forensic	This describes scientific methods used to investigate crimes (Carrier, 2004).

LIST OF ABBREVIATIONS AND ACRONYMS

ACPO	–	Association of Chief Police Officers
BIOS	–	Basic Input Output System
CID	–	Criminal Investigation Department
CSS3	–	Cascaded Style Sheets version 3
DCI	–	Directorate of Criminal Investigation
FBI	–	Federal Bureau of Investigation
HRM	–	Human Resource Management
HTML	–	Hypertext Mark-up Language
ICT	–	Information and Communication Technologies
IT	–	Information Technology
PHP	–	Hypertext Pre-processor
RAM	–	Random Access Memory
XAMPP	–	Cross-Platform Apache, MySQL, PHP and Perl
SOPs	–	Standard Operation Procedures

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter introduces the research study, presents the statement of the problem, research objectives and significance of the study as well as the scope of the research study.

Many things have been written and done in improving the viability of digital law enforcement as pertained to the earlier failures. The Federal Bureau of Investigation (FBI) has a network of computer crime squads. The Justice Department has set up a set of strategies outlining measures for seizing and searching the computers. The general US population are more educated on computer crime, and many do know what to do so as to protect themselves (Cole, Smith, & DeJong, 2018).

1.2 Background to the Study

New developments in the digital world challenge law enforcement, legal and judicial professionals to maintain current proficiencies concerning legal issues and technical aspects in the rapidly changing environment. Digital crime encompasses not only new crimes but also those that have been in existence committed using digital techniques. The boundaries of forensic science are expanding, and so is the need for trained professionals. The centre of excellence in digital forensics provides a mechanism to meet these challenges. Police agencies typically use either Encase or Forensic Toolkit to do their forensic evaluation of the client's hard drives (Taylor *et al.*, 2014). The established forensic tools, during investigations are limited by their inability to preserve the hardware and software state. Investigators do shut down the machine so as to inspect the contents of the disk and identify the artefact of interest. This process breaks the network connections and also unmounts encrypted disks in computers causing significant loss of evidence and possibility of disruption of critical systems (Taveras, 2013).

In recent years, it has come to a realization that only trying to prevent information technology incidents is insufficient, as literature shows that a determined attacker with sufficient resources will finally succeed in breaking or circumventing the measures taken. As such, organizations are taking a more holistic approach to information security, detective, implementing preventive and taking responsive measures (Fielder *et al.*, 2016). There are underlying reasons that demand we pay more attention to the cybercrime and our capacity

assistance in investigating and prosecuting cyber offenders (Kshetri, 2013). The laws written before computer forensics era are normally obsolete and therefore they cannot effectively weigh up the procedures used in a computer system search. Incapability of the law keeping in pace with the technological progression could in the long run limit the usage of computer forensics evidence in the courts. The approval and growth of digital forensics in Kenya has been very slow because of the inappropriate regulatory policies, technologies, standards, procedures, legal and governance challenges. The law ought to keep pace with the advancement of the technology for the progress of computer forensics

According to Douglas *et al.*, (2013), many crimes that had gone unsolved are now being solved with the help of forensic science in identifying the perpetrators. However, these advances have also revealed that, in some cases some of the testimonies and information based on faulty forensic science analyses may have contributed to wrongful convictions of innocent people. This has demonstrated potential danger of giving unjustified weight to evidence and testimony derived from imperfect testing and analysis. Furthermore, exaggerated expert testimonies sometimes have contributed to the admission of incorrect or deceptive evidence.

In Australia, Caelli and Liu (2018) notes that the law requires that expert evidence meet a standard of evidentiary reliability, that is, the specialised knowledge be "sufficiently recognised to be accepted as a reliable body of knowledge or experience". The second requirement in Australian law is that the witness has the required specialised knowledge by demonstrating appropriate qualifications and experience. Cumins (2016) remarks that in computer forensics, there were still no formal expert accreditation available. Some private institutions offer computer forensics training, and many offer vendor specific software training. While such trainings were useful they were not seen as leading to a recognized certification. A similar situation is prevalent in other technologically advanced countries. The first prosecuted computer crime case took place in 1966, and the first computer forensics training course appeared around 1989 at University of North Texas

The Canadian government has been very aggressive in realization of computer crime legislation. There are two sections in the Canadian criminal code, sections 430 and 342.1 that deal with computer crime. Section 342.1 is divided into two parts. The first part contains items forensically considered as computer crime. This identifies unlawful entry into systems, interruption of transmissions, and mandating an insensitive ten year sentence in prison for

violating the laws. The second part identifies computer programs or data that gives documentation as to what kind of materials would meet the criteria under the law. Section 430 criminalizes actual destruction, interruption of data, data transmission or alteration (Fraser, 2017).

A very crucial unit of the Kenya Police is the Directorate of Criminal Investigation (DCI) Kenya which is commonly known as the Criminal Investigation Department (CID). This unit does very complex investigations and high profile cases and therefore require high end expertise. The headquarters is situated in Nairobi along Kiambu road. The unit has branches in all the counties across the Republic of Kenya. The CID also have made work easier by having subunits like the Flying squad, Anti-banking fraud unit, Special crime prevention units, Anti-terrorism Police Unit (ATPU), Ballistic unit, Anti-narcotics unit, Bomb squad, cyber forensics, and forensics department. All this help in contribution of the success and competence in the units they are. They collect and provide criminal intelligence, investigate serious crimes, do forensic analysis and as well coordinate the county Interpol affairs among others (Hope, 2018).

In Kenya, the police investigate crimes related to computer systems and data (Throup, 2017). Some of the examples of the crimes are illegal access; investigating crimes committed through or by means of computer systems like child pornography; finding, recovering, analyzing and evaluating digital data by using a collection of tools or ways for discovering digital data that exist in a particular medium; criminal and administrative matters in protecting users and resources from exploitation, invasion of privacy; sensitizing police officers and members of public on matters relating to cyber-crimes; supporting investigative units of the police in collection of electronic evidence through forensic analysis of digital media; providing technical cyber investigation capabilities to support criminal investigations and immediate response to incidences to collect volatile data; giving unbiased scientific evidence and expert belief in court; mentoring, coaching and appraising officers and doing research on new techniques and methodologies relevant to cybercrime investigation work. There are issues that have restricted access of quality policing service. This are; delay to scene of crime, low rate of crime detection and prevention, poor crime scene management, lack of adequate resources and lack of proper human resource management (HRM) policy and systems.

1.3 Statement of the Problem

The growing incidence and risk of inappropriate, illegal and/or criminal computer behaviours increases the need to build bridges between technical and legal areas of expertise. This is in order to produce more effective defensive and offensive responses. Although there are already large volumes of literature on organizational, technical and legal issues pertaining to computer misuse and e-crime, there have until recently been only limited explorations of the interrelationships between these issues. This has been mostly because of the complexity of the specific sets of legal and technical challenges faced (Hannan *et al.*, 2003).

Kadish *et al.*, (2016) notes that in legal cases evidence is either admitted or not depending on the relative weight of its probative and prejudicial value. In Kenya, digital forensics process is often faced with challenges like admissibility, accuracy, authenticity, relevancy, reliability and convincing to juries. This is because of poor standards like ISO 17799 and COBIT, regulatory policies, governance and technologies.

At present, the tools used in computer forensic are incapable of presenting a visual overview of the total data found on storage media. This impression could prove vital in digital investigation. The problem of this research was fulfilled through the extensive review of the associated literature with respect to the analysis done by the researcher. The following research questions were addressed; what were the current technologies in place and the contribution of legal framework, regulatory policies towards admissibility of digital forensics; what components could make up a forensically sound digital data acquisition process; and the effectiveness of digital forensics in digital crime handling? As the volume of data to be analysed continues to grow, digital investigations become more complex and time consuming (Hashem *et al.*, 2015).

1.4 Purpose of the Study

The study intended to provide a means for the Kenya Police Service in evaluating their forensic adoptability in digital forensic evidence.

1.5 Objectives of the Study

The main objective of this research was to investigate the adoptability of digital forensics in digital crime handling in Kenya.

1.5.1 Specific Objectives

- i. To investigate the effectiveness of digital forensics in digital crime handling in Kenya police service.
- ii. To investigate contribution of technology, legal framework and regulatory policies towards admissibility of digital forensics.
- iii. To examine the essential components that will make up a forensically sound digital data acquisition process.
- iv. To develop an adoptability model for application of digital forensic.

1.6 Research Questions

- i. How will the effectiveness of digital forensics in digital crime handling in Kenya Police Service be investigated?
- ii. How do technology, legal framework, regulatory policies and practices contribute towards admissibility of digital forensics?
- iii. What are the essential components that make up forensically sound digital data acquisition process?
- iv. How can the adoptability model be developed?

1.7 Significance of the Study

The study was intended for those who were operating in the fields of computer forensics who are experts, trained and already have the necessary skills and experience for undertaking forensics. For the other researchers, it can be used as a blueprint. The study aimed at informing policy development in the Kenya Police Service in forensic evidence handling. The study was to assist in improving the handling methods implemented in the law enforcement and incident response teams. It was supposed to help in making good choices of forensic tools equipment in investigation procedures. The study would aid in easy movement of digital evidence throughout the chain of custody. The findings were also to bring about a reduction of costs incurred in carrying out digital forensic activities. This could be due to the use of inappropriate tools for evidence handling. Less time could be taken to carry out digital evidence activities. This study formed a basis for further research in new areas in digital evidence forensics and its effects on organizations. It should guide scholars who may be interested in doing a research in a similar field. Both the experimental and theoretical results of this study would help scholars as they investigate on digital evidence acquisition functions and the chain of custody at large.

1.8 Scope of the Study

The research targeted Kenya Police Service county offices across the country. Nakuru County Police Service acting as a representative of the forty seven counties in the country during the collection of data.

1.9 Limitations of the Study

The researcher might not be given all the necessary information or data needed as some are kept confidential by the law enforcement. Giving out of information by the respondents was also hard since many did fear victimization. This problem was solved by obtaining an authorization letter from the concerned authorities and allowed the respondents feel free in giving information. Attached is Appendix VI, showing the authorization letter.

1.10 Assumptions of the Study

It was assumed that since the research was involving government officers, that there would be total cooperation in provision of information from the targeted organization. The researcher also assumed that the police service would positively accept the adoptability model for digital forensic evidence.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter discusses the review of theoretical literature relating to the investigation of digital forensic evidence which includes the review of critical literature and identification of the gaps to be filled, summary of the literature reviewed and the conceptual framework.

2.2 Digital Forensic

Computer technology is the major important part of daily human life and growing rapidly fast, and as the technology grows, the computer crimes such as unlawful intrusion, financial fraud, identity and intellectual theft also increase. To counteract these computer-related crimes, computer forensics plays a very important role. Computer forensics involves acquiring and analysing digital information for use as evidence in criminal, civil or administrative cases (Soltani & Seno, 2017). Computer forensics is a branch of digital forensics that use analysis techniques to gather potential evidence from desktops, laptops and server computers for investigating suspected illegal or unauthorized activities. More precisely, computer forensics focused on finding potential digital evidence after a computer security incident has occurred (Crouch, 2012). Computer Forensics is an emerging field and there is less standardization and consistency across the courts and industry (Walsh, 2018). Each of the computer forensic methods is focused on particular areas such as electronic evidence discovery or law enforcement. There has never been a single digital forensic investigation technique that has been accepted universally. However, it was generally accepted that the digital forensic technique must be flexible, in that it can support any type of incidents and the new technologies (Adam, 2013).

Digital forensics is a branch of forensic science often related to computer crime, and includes investigation and recovery of materials which are found in digital devices (Pichan, Lazarescu, & Soh, 2015). Casey (2011) says digital forensics deals with the application of scientific knowledge for collecting, analyzing, and presenting legal evidence. Digital evidence, in its nature is extremely fragile therefore; it can be easily altered, damaged or even destroyed by inappropriate handling or examination. For these reasons high precautions ought to be taken to safeguard this type of evidence. Failure to do so could render it unusable or lead to an inaccurate conclusion. The production of computers and mobile phones in our societies is at

its rise. The worldwide mobile phone subscriber base has reached around 4.4 billion. Almost two thirds of the worldwide population currently use mobile phone (Zhang *et al.*, 2015).

2.3 Effectiveness of Digital Forensic in Digital Crime Handling

According to Grobler, Louwrens and Solm (2010), digital forensic is deemed effective if it has the ability to produce desired results. The performance of digital forensic tools presents different strengths and weaknesses as opposed to their declared capabilities.

2.3.1 Digital Crime Handling

Traditionally, to collect the physical drive, the United States Secret Service recommends the investigators to pull out the power plug from the computer (United States Secret Service, 2010). The power of the computer and the hard drive is cut down and this prevents erasing of data from the drive. The hard drive preserves the data. In examining the data, the suspect's drive is connected to a write blocker after being removed from the computer. This prevents changing of data in the suspect's drive (Carrier, 2010). The investigator then creates an image file that is an exact copy of the drive by using specialized software. By use of MD5 hash values, the investigator can confirm the copy as the same (NIST, 2006). If the hash value matches with the new copy, then it is successful.

As per the tradition, to prevent anyone from accessing systems from outside the crime scene, it is generally advisable to disable network connectivity to all computer systems, which is currently done, but in doing so, evidence can be destroyed and will eliminate investigative opportunities. The hardware and software state will not be preserved and by not being able to respond effectively could be extremely damaging especially to small organizations which could not absorb losses easily as in large organizations (Kim & Solomon, 2016). Checkland and Poulter (2006) consider a real-world problematic situation that requires some form of intervention in order to improve it. This intervention requires the identification and analysis of a given problem situation by a researcher to develop a deep understanding of the problem area in order that an appropriate solution can be identified.

According to Hossain, Hasan, and Skjellum (2017), the first responder must have permission first from the authority; like plain view observation, consent, or a court order, to search and collect evidence at an electronic crime scene. The guidelines, consultation of a superior or contacting of a prosecutor if a question of appropriate authority arises will be followed. Digital evidence must be handled carefully to preserve the integrity of the physical device as

well as the data it contains. Electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices can damage or alter data. To preserve the integrity of the physical device and the data contained, careful handling should be maintained. Data may become inaccessible if data encryption is in use on a computer or data storage device that is improperly powered off during digital evidence collection. Removing the power supply when you identify a computer is usually the safest decision if evidence of a crime is visible on the computer display (Ballou, 2010).

According to Hoffman and Zefferet, any party who wishes to rely upon statements contained in a document, must ordinarily comply with three general rules: i) Subject to various exceptions, the contents of document may be proved only by production of the original (best evidence rule); ii) Evidence is normally required to satisfy the court of the documents authenticity, also subject to various exclusions iii) A document may have to be stamped in accordance with the Stamp Duties Act 1968. Thus this information, though in the form of a data message, will be given due evidential weight, having regard to: the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which the integrity of the data message was maintained; the manner in which its originator will be identified; and any other relevant factor (Lubaale, 2015; Bokolo, 2014).

The internet economy of the UK is among the world's strongest therefore, the cyber criminals both domestic and international do view UK based businesses and other private individuals as the best targets for the cyber-crime. In tackling of the cyber-crime, the UK law enforcement work in partnership with the NCA's (National Cyber Crime Unit) that leads the response of cyber-crime, City of London Police that do provide Action Fraud reporting service, Metropolitan Police, Regional Organised Crime Units and the Police Forces across the country (National Crime Agency, 2016).

For a long time, the lack of a forensic laboratory has made it hard for police in Kenya to prosecute terror and other criminal cases (Fred Mukinda, July 10 2016 Daily Nation). It makes the police independent when carrying out DNA, ballistic and explosives analysis. At present, they rely on the Government Chemist at Kenyatta National Hospital for biological and chemical analysis and in complex DNA cases; they seek help abroad, mostly South Africa and Europe.

2.3.2 Digital Forensics in Law

There is an increase in the use of digital forensics in courts mostly in the overseas countries like Australia. The court's role is to provide a forum for resolution of legal disputes between the individual and the government (Howard, 2014). Facts of a case presented by both parties in a dispute are tendered as evidence. This evidence can be categorised into eyewitness, which is the one seen by a person; circumstantial, which is the information used in making inference and the expert, which are the opinions based on the knowledge of the expert himself.

Previous studies have shown that developing countries have not yet derived expected benefits from digital forensic technology as very few organizations have the structures in place to enable them to conduct cost effective, low-impact and efficient digital investigations. In Kenya, the adoption, maturation and proliferation of digital forensics is slow due to inappropriate regulatory policies, procedures/processes, standards, technologies, legal and governance challenges (Moturi, 2011).

2.3.3 Effectiveness of Digital Forensic in Kenya

The laws which were written earlier than the computer forensics era are normally outdated and therefore, cannot effectively assess the procedures used in a computer system search. The incapability of the law keeping in pace with the technological advancements could eventually limit the usage of computer forensics evidence in the court. The acceptance and development of digital forensics in Kenya has been very slow because of the inappropriate regulatory policies, standards, procedures, technologies, and legal and governance challenges. For the progress of computer forensics, the law ought to keep pace with the advancement of the technology. The challenge in Kenya is training. Lack of training led to vulnerability of court dismissal as there is failure in protecting organizations in the event of disputes. This ineffectiveness is worthy as it goes a long way in enhancement of computer forensic capacity in Kenya. Hope (2018) further states that in countries that the police corruption is persistent, like Kenya, there is a representation of a general failure of the governance. This is where the main institutions in charge of ensuring police accountability, observance of ethics and integrity standards and the enforcement of the rule of law are compromised and infested with corrupt individuals.

In 2004, Sam Houston State University established the Centre of Excellence in Digital Forensics. The centre is dedicated to preparing digital forensics professions through teaching, training and research. The centre of excellence in digital forensic has a dedication to developing new approach in the detection, preservation and analysis of digital evidence. The centre also provides databases to facilitate digital forensic profiling, digital fraud investigation. It maintains software and hardware tools to improve data detection / recovery and network security.

2.4 Contribution of Technology, Legal Framework and Regulatory Policies towards Admissibility of Digital Forensics

Majority of jurisdictions do have legal requirements that offer grounds of digital evidence admissibility in legal proceedings. The rapid advancement of technologies, the increased globalization of the virtual environment and the reactive nature of the countries regulatory process complicates the research as it continues to evolve and as the field continues to mature (Jin, 2017).

2.4.1 Chain of Custody

The chain of custody refers to the requirement that an item of evidence be proved to be genuine to the level its proponent claims it to be. Cosic and Baca (2010), also give another definition as the chronological documentation or paper trail, showing the paper trail, custody, control, transfer, analysis, and disposition of physical or electronic evidence. This starts exactly the moment of the entry to the crime scene till the end of the court case. Documenting each and every change in the evidence and assessing in perspective of the final analytical results (Casey, 2007). This is the basic part of the validity of the case and the forensic soundness of the evidence. According to Dykstra and Sherman (2012), chain of custody is authentication or identification of real evidence (that is; tangible evidence that is historically connected with a criminal case and not merely illustrative).

2.4.2 Legal Aspect

Legal implications are there and any person who is involved in any activity of forensic should be aware of like having authorization before monitoring or collecting of information or data in digital forensics. All the time more laws are passed to safeguard privacy of information for organizations. There are three areas that one should know about in law relates which are; the statutory laws affecting one, safeguard against perverse search and seizure; protection against self-incrimination and lastly understanding about hearsay, reliability, authentication and best

evidence. Violation of these leads to federal felony which is punishable by fine or imprisonment (US CERT, 2008).

2.4.3 Digital Forensics Security Fundamentals

According to Saks and Koehler (2005), we are in a theory shift in 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. Peltier (2013) notes that the core IT Security fundamentals to digital forensics are; Confidentiality, Integrity and Availability (CIA) as illustrated in Figure 1.



Figure 1: Information Security Management

(Source: Peltier, 2013)

2.4.4 Threat Intelligence

Weedon, Nuland and Stamos (2017) states that threat intelligence helped to identify the vulnerabilities and the newly discovered threats, identifying stolen data and the past compromise. The correlation of various data sources using analytical methods can also be used to discover incidents that were not otherwise detected. With the ISO 27005, it helped cover the flaws in the 27K by dealing with the information risk management. Threat intelligence enables organizations stay one step ahead of threats.

2.4.5 Code of Ethics

As the technology and the tools are becoming more persistent, information can be maintained longer, since more people have easier access to sensitive incident data over a lengthy period of time. According to ISO/IEC 17025:2005, *accreditation of the digital forensics discipline*,

the expert in digital forensics should act with competence and integrity. Confidentiality should be highly preserved and evading of any action that might be a conflict of interest.

2.4.6 Technologies Used in Forensic

Technologies such as Digital Surveillance for Xbox (XFT) device is useful as the XFT sessions can later be replayed during court hearings in real time. This toolkit allowed law enforcement agencies to scour the inbuilt hard disk of such devices and find illicit hidden materials easily (Xynos *et al.*, 2010). It was developed to allow authorities visual access to hidden files on the Xbox hard drive. Kaur, Saini and Sood (2013) states that the investigators used a Video Spectral Comparator 2000 device to look at pieces of paper in case there were any hidden or obscured writing, that one could determine the quality of the paper and analysis done even if the paper was damaged by fire or water.

2.4.7 Guidelines and Principles

Guidelines for handling digital evidence in law enforcement agencies are very important. In a crime scene, broad analysis and correct handling of the digital evidence should be considered for right presentation in the court (Lutui, 2016).

2.4.7.1 ISO/IEC 27037:2012

Computer forensic practitioners and scientists are regularly expected to meet specific standards in order to satisfy the legal authorities. According to Guarino (2013), the ISO / IEC 27037 standards present the guidelines for identifying, collecting, acquiring and preserving of digital evidence. Prior to the release of ISO/IEC 27037, there were no globally-accepted standards on acquiring digital evidence. Police developed their own national guidelines and procedures for the acquisition and protection of electronic evidence (Drucker, 2017). However with this, it creates issues in case of cross-border crimes. This happens when digital forensic evidence acquired in one country needs to be presented in the courts of another. Tainted evidence that may have been acquired or protected without the requisite level of security may be legally inadmissible. For the widest applicability, ISO standards will not mandate the use of particular tools or methods. ISO 27043 standard permits forensic practitioners to perform any action provided it can be justified in court. The ISO 272 standard directs the field of forensic and gives uniformity and reliability in collection, analysis, storage and retrieval of the forensic evidence.

2.4.7.2 Association of Chief Police Officers (ACPO)

This research was conducted as per the Association of Chief Police Officers (ACPO) guidelines and also its four principles. The Association of Chief Police Officers (ACPO) advises the forensic practitioners through the guidelines offered that in exceptional situations where a person sees a necessity in accessing original data which is held on a storage media or a computer, that person should be proficient in doing so and able to prove the relevance and the outcome of their act (Eales, 2016).

Principle 1: The data stored in the computer should not be altered or changed, as they can be later presented in the court; *Principle 2:* The Person handling the original computer data should be competent enough, and shall also be able to give the evidence explaining the relevance and course of their actions; *Principle 3:* The documentations and audit trail for the procedures applied to computer-based electronic evidence should be created and preserved in that any other person should be able to scrutinize those processes and attain same result; *Principle 4:* The person who is responsible for the investigation will have an overall responsibility for accounting that the law and the ACPO principles are adhered to.

Soltani and Seno (2017) developed a basic digital forensic investigation process called the Four Step Forensics Process (FSFP) with Venter (2006) idea that digital forensics investigation can be conducted by even non-technical persons. This process gives more flexibility than any other method so that an organization can adopt the most suitable method based on the situations that occurred. From the final report and recommendations of Article 19, legal analysis of the Kenya's 'Cyber-crime and Computer Related Crimes Bill', it is conclusively right to say there is need to review bills & laws that involve the use of digital evidence in court. The need to unite legislators, law enforcement agencies and privacy advocates, groups together and come up with sound Standard Operation Procedures (SOPs) for Forensics examiners as well as laws that can assist in having a fair and unbiased trial (Saini, Rao & Panda, 2012).

2.4.8 Approach for Creation of Cyber Laws

Cyber laws ensure smooth governance of the internet across the world (Manish, 2013). Manish further explains that the following assist in creation of cyber laws.: formulating new laws and amendment of the already existing laws by the nations in their territory that have impact on their own; entering international multilateral agreements to have uniform rules and

creating new international organisation, that will establish new rules and the means of enforcing them.

2.4.9 Constitutional Law

Soliciting a minor by the use of a computer for sex is always considered a crime by the state (Brenner, 2001). Several rulings states that the offense is committed if the person behind it believes he was soliciting a minor for sex, even though it's not true (Texas Penal Code 15.031). They are also reliable in prohibiting the use of computers to possess, create, and/or distribute child pornography (Brenner, 2001). Many countries like Australia, India, UK, Malaysia, Turkey, Switzerland, Canada, USA, Denmark, Greece, Japan, Finland, Austria, Portugal, Singapore, Spain, Italy, Germany, Sweden and Malaysia have reconsidered their own criminal laws in order to prevent the computer related crimes. However, there is no country that has fully resolved all issues such as the legal, enforcement and prevention of crime. The legislation enacted covers few of the classified computer related offences (Manish, 2013).

India has a detailed and well defined legal systems in place and with Indian Penal code laws, the Banker's Book evidence Act, 1891, Indian Evidence Act 1872, the Companies Act and the Reserve Bank of India Act, 1934 and more. During enactment, nobody really visualised about the internet. Like the rest of the world, the existing laws in India could not handle various cyber space activities, and therefore the need of a cyber law arose.

2.4.10 Challenges in Law Enforcement

New developments in the digital world challenge law enforcement, legal and judicial professionals to maintain current proficiencies concerning legal issues and technical aspects in the rapidly changing environment. Digital crime encompasses not only new crimes but traditional crimes committed using digital techniques. The boundaries of forensic science are expanding, and so is the need for trained professionals. The centre of excellence in digital forensics provides a mechanism to meet these challenges. Police agencies typically use either Encase or Forensic Toolkit to do their forensic evaluation of your client's hard drives (Taylor, Fritsch & Liederbach, 2014).

There are common issues facing current law enforcement. These are; politicians do abuse the police with their personal agendas, recruitment is done through politics and the oversight bodies are partisan, training do not address all required elements and therefore the recruits are

not well educated on intake, the forces are understaffed, inadequate communication and transport infrastructures, inadequate evidence handling and forensic capacities. Due to poor pay as well as conditions, it leads the police in accepting bribes; therefore efforts to address corruption are inadequate and inconsistent. There are human rights violations and community policing is frustrated by lack of trust and therefore public perception of the police is highly negative (Simon, 2009).

2.5 Components for Forensically Sound Digital Data Acquisition

Overill and Chow (2018) argues that, for evidence to be forensically sound, the disk image must be an exact copy of the original one. The disk image process must include a means for verifying the authenticity and also the reliability of the copying process.

2.5.1 Tools and Materials for Collecting Digital Evidence

There are tools for processing crime scenes that are used and in addition, the first responders should have the following items in their digital evidence collection toolkit: Cameras both photo and video, Gloves, Cardboard boxes, Notepads, Evidence inventory logs, Crime scene tape, Evidence tape, Evidence stickers, labels or tags, Antistatic bags, Permanent markers, Paper evidence bags and Non-magnetic tools (Ballou, 2010). The following are Tables 1, 2 and 3 showing a summary of some tools and its functions, division of the tools either static or live and comparison between live and static tools respectively.

Table 1: Comparison of Forensic Tools Function

Function	ProDiscover Basic	OSForensics, demo version	Access Data FTK	Guidance Software EnCase
Acquisition				
Physical data copy	√	√	√	√
Logical data copy	√	√	√	
Data acquisition formats	√	√	√	√
Command-line processes				√
GUI processes	√	√	√	√
Remote acquisition		√	√	√
Validation and verification				
Hashing	√	√	√	√

Verification	√	√	√	√
Filtering		√	√	√
Analyzing file headers		√	√	√
Extraction				
Data viewing	√	√	√	√
Keyword searching	√	√	√	√
Decompressing			√	√
Carving		√	√	√
Decrypting		√	√	
Bookmarking	√	√	√	√
Reconstruction				
Disk-to-disk copy	√	√	√	√
Partition-to-partition copy	√	√	√	√
Image-to-disk copy	√	√	√	√
Image-to-partition copy	√	√	√	√
Disk-to-image copy	√	√	√	√
Rebuilding files	√	√	√	√
Reporting				
Bookmarking / tagging	√	√	√	√
Log reports		√	√	√
Report generator	√	√	√	
Automation and other features				
Scripting language				√
Mount virtual machines		√	√	√
E-discovery		√	√	√

(Source: Nelson, Phillips & Steuart, 2014)

Table 1 is a list of some of the computer forensic tools and their functions. A tick (√) mark represents where a particular function is available in the tool. As observed, the computer forensic tools are unable to present an impression for all the data found on a media device.

Table 2: Exploring Static and Live Digital Forensics: Methods, Practices and Tools

Sr. No	Tool Name	Op Sys	Purpose/Description	Static/ Live Analysis
1.	Registry Recon	Windows	This tool is used to rebuild the registries of Windows from any place of a hard drive and further it is parsed for the analysis in depth.	Static
2.	SIFT (SANS Investigative Forensics Toolkit)	Ubuntu	SIFT is used to perform digital forensic analysis on different operating system.	Live
3.	EnCase	Windows	This tool is used to gather and analyze memory dump in digital forensic investigation in static mode	Static
4.	Digital Forensics Framework	Windows/ Linux/ Mac OS	During the live and static analysis, DFF is utilized as a development platform and digital investigation tool.	Both
5.	EPRB (Elcom soft Password Recovery Bundle)	Windows	This toolkit is used to perform digital analysis on encrypted system, password recovery and data decryption.	Live

6.	PTK Forensics (Programmers Toolkit)	LAMP	It is GUI based framework for static and live analysis.	Both
7.	FTK (Forensic Toolkit)	Windows	This tool is used to perform digital analysis and indexing the evidentiary data.	Static
8.	The Coroner's Toolkit	Unix	It is a command line user interface tool to perform forensic analysis on Unix systems.	Both
9.	The Sleuth Kit	Unix/Wind ows	Toolkit provides GUI and command line interface to per-form digital forensic analysis in Unix and windows.	Live
10.	COFEE (Computer online forensic evidence extractor)	Windows	COFEE is used to extract and analyze forensic data lively.	Live
11.	OCFA (Open Computer Forensics Architecture)	Linux	It is a command line interface for distributed computer forensics and it is used to analyze digital media. It is mostly used in digital forensic labs.	Live
12.	OS Forensics	Windows	This tool is used to perform analysis on E-mail, Files, Images and web browsers.	Live

14.	Safe Back	Windows	This tool is used for evidence collection, analysis and for creating backup of evidentiary data in digital media.	Static
15.	Forensic Assistant	Windows	It is used to analyze the activities performed by user on internet like emails, docs and IM and web browsers.	Live
16.	X-Way Forensics	Windows	This tool is used for the general purpose on Win Hex editor used to perform static and live analysis.	Both
17.	CAINE (Computer Aided investigative environment)	Linux	Command line user interface used for distributed and standalone computer forensics.	Both
18.	bulk extractor	Windows, Linux	For the extraction of phone numbers, email addresses, URLs and the other objects which are identified.	Live
19.	IRCR (Incident Response Collection Report)	Windows	Collects live forensics information from the command history, computer, network connection,	Live

			current processes, opened ports, registry start up information and event logs from system.	
20.	Intella	Windows	It is used to process and investigate Email, digital data and Cell phones.	Live
21.	CMAT(Compile Memory Analysis Tool)	Windows	It extracts information from the memory dump and also exposes malware.	Live
22.	WFT (Window Forensic Toolkit)	Windows	Toolkit used to analyze the memory, system information, file/directory timestamp, port number, user information,	Live

(Source: Rafique, & Khan, 2013).

Table 3: Comparison of Traditional Forensic Versus Live Forensic

Traditional/static forensic	Live forensic
This is performed on dead systems	This is performed on running system
The moment the computer is unplugged, volatile memory in the RAM is lost. Therefore it can't acquire live or volatile data.	They do acquire live data
Temporary data is lost	Temporary data is analysed for the likelihood of evidence.
They first wait for something to fail for them	Automation is adopted. The digital devices

to fix it, which results to low productivity as it takes longer time.	focus on resources, identify and collect possible evidence.
All data for evidence must be gathered and examined to be able to comply with the requirements for traditional forensic thereby complicating the investigation process.	They limit the data to be collected. The large parts are investigated and only relevant pieces of information are gathered.
It becomes of no use if the hard drive is encrypted even if the investigator has the entire bit for bit hard drive image of the supposed system.	The investigators can be able to access the disk if same encrypted disk is acquired.
This is a reactive approach	This is a proactive approach

(Source: Rahman & Khan, 2015).

Live analysis on a running system can be used to obtain volatile data to understand events that had occurred in the past (Mrdovic *et al.*, 2009). Running systems are incapable of being reversed and they change their state by making collected evidence invalid.

2.5.2 The Cyber Tools On-Line Search for Evidence (CTOSE).

Cyber Tools On-Line Search for Evidence (CTOSE) developed a methodology that aims to provide a consistent approach for identifying, preserving, analyzing and presenting digital evidence. The focus of the CTOSE is on the acquisition of digital evidence and on how it is to be collected, conserved and analyzed in a manner that is legally admissible should court proceedings be brought about. However, its context is primarily that of IT security management for network administrators rather than a FC tool per se (Slay, *et al.* 2004). The disadvantage in this is that it is not designed with the need to track, trace and generate legally admissible evidence about these behaviours. There is also a growing awareness that most computer security systems can easily be tainted and their evidence contaminated.

2.5.3 Components that May Cause Inadmissibility of Evidence

According to Jansen and Grance, (2011), during accessing of a live machine in digital evidence, the researcher would not only access the building of where the evidence is deemed but will also look at the machine passwords or usernames, thereby might bring complications.

Any modification of the data can cause inadmissibility of evidence in court. Jones (2008) notes that in live forensics, each of the operating systems needs to be treated differently

during investigation as it can cause practical problems since interaction with the suspect's machine operating system is needed. Lessing and Von Solms (2008), further states that authentication of every value should be done before the court can accept it as legit evidence. The judicial systems have not been in acceptance with the digital evidence and computer technology. It needs courts extensive knowledge of all new technological developments.

2.5.4 Digital Forensic Processes

Investigation is done in order to realise an incidence triggered by the detection of irregularities in a system, information about a crime and so on (Oriwoh, & Williams, 2015). Wilding (2017) argues that in any scene of a suspected fraud or computer misuse, there is usually a range of apparently irrelevant items that might be important and which are worth attention. Most of these potential sources of evidence are unrelated to the computer systems, but they are all worthy to be considered. Search and seizure of digital evidence is the first procedure that is mostly disputed in courts. During this initial process of forensic investigation, the use of an improper methodology or unlawful search and seizure can negatively affect the admissibility of the evidence (Cole *et al.*, 2015). Adoption of a good strategy would maximize collection of untainted evidence and minimize impact on the victim.

According to Tajuddin and Manaf (2015), digital evidence can be very fragile and naturally it has several challenges unlike evidence encountered during traditional investigations. When the system is shut down; the memory resident programs can be lost, they can be manipulated or altered without having a trace during the collection, analysis and presentation. Oriwoh and Williams (2015) says that a systematic search of evidence about the incident being investigated is done. This is by examining of computer media, such as floppy disks, hard disk drives, backup tapes, CD-ROM's and any other media used to store data. Evidence analysis is required to identify the perpetrator of crime, claim damages and defend copyrights. It involves determining significance, reconstructing data fragments of data and drawing some conclusions based on the evidence collected. Evidence analysis may require the use of tools and tests to be done more than once to support the crime theory. Technical knowledge is required to undertake an effective analysis process (Robertson, Vignaux, & Berger, 2016). Reporting which involves translating, summarising and giving some conclusions on the analysis of the evidence becomes the last stage.

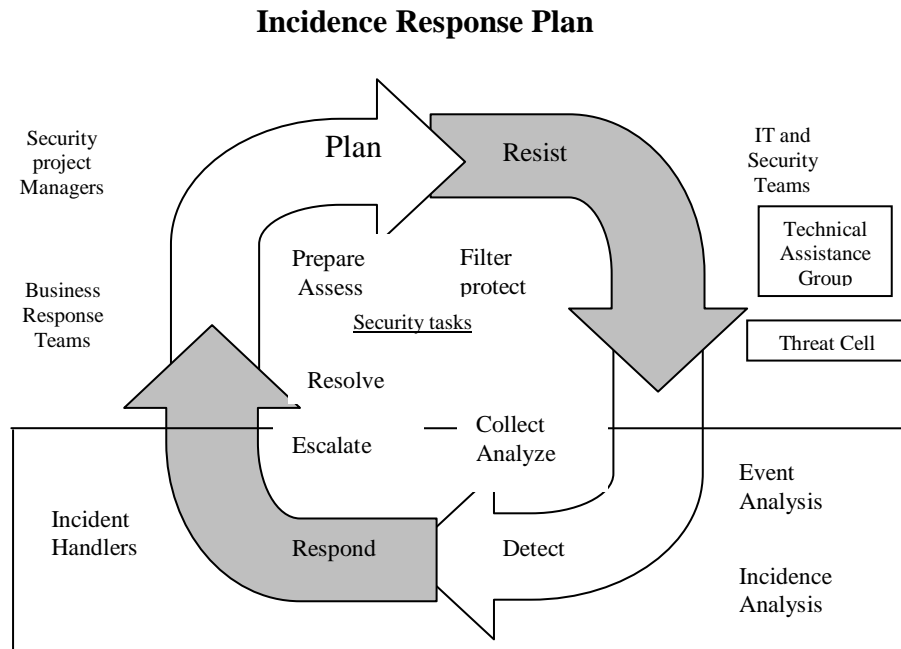


Figure 2: CIRT-Level Response to Advanced Persistent threat

Source: (Richard, 2006)

An incident response plan is a well organized and documented process of how to approach and manage situations that results from information technology security events. According to Richard (2006), the CIRT-Level Response to Advanced Persistent threat has four stages name; i) *Plan*: The security posture is assessed, understanding of the threat and the extent of the vulnerability of the threat. Organization’s designs effective, practical and relevant information security. ii) *Resist*: The organization resists attacks when it plans its defence tactics and strategies, and deploys the appropriate components of its security architecture. This involves using security technologies, with the right processes in place, to filter unwanted network traffic in both inbound and outbound directions, block exploits and malware infections (to the extent possible), control access to data, guard web applications, and so on. iii) *Detect*: When a file is deleted in a computer, the computer knows that you no longer have interest in it and can’t go finding all the other pieces of the file, therefore removes all the contents from the table of contents and nothing is physically deleted at that point. The data will still exist in the computer’s hard drive though the operating system will be reporting that the data is already deleted and no longer exist. The forensic experts who can use the disk snooping tools can use this data for inspection. It doesn’t bother to go out and find all the pieces again because it knows that you’re no longer interested in all the pieces (Fallows, 2008). iv) *Response*: After detection, the organization mobilizes its incident handlers to

respond to the intrusion. This process typically involves understanding the incident's scope, containing the situation, eradicating the attacker's presence and recovering from the incident (Chike, 2016). The post incident activity, in the form of lessons learned, provides input to the *plan* phase of the cycle.

2.5.5 Steps in Digital Evidence Acquisition

According to Moreau and Dale (2013), primary theoretical aspect of crime scene photography is the notion that in order to adequately exhibit the crime scene, a sequence of photographs showing all pertinent locations in an organized manner must be compiled. As a basic guideline, the subject matter encountered is to be represented by a progression of "general to specific." This circumstance involve the coverage of the crime scene from three major vantage points i) long-range ii) mid-range and iii) close-up. The acquisition of photographs to document this coverage applies not only to the crime scene location as a whole, but also to each segment of the scene investigation.

During photography in the crime scene, it is the responsibility of the photographer to attain a basis of knowledge which would help explore the "who, what, when and where" of the situation. If these aspects are not thoroughly examined and understood the photographic product of a crime scene can actually harm the prosecution of a case. "Raking-pictures" is one thing while photographically documenting a crime scene for logical and convincing display to a jury is another. The person holding the camera must necessarily be aware of the theory of crime scene photography, which is combined with the practical and equipment operation segments of the task. Only when theory and practice have been integrated will success be complete (Moreau & Dale, 2013). The final stage in scene documentation is making a sketch of the crime scene. The disadvantage of the photographs is that they represent two-dimension of three-dimensional objects (Becker, 2005).

Evidence handling was one of the main aspects in the expanding field of computer forensics. Corrigan (2007) notes that one of the more recent shifts in evidence handling was the shift away from simply "pulling the plug" as a first step in evidence collection to the adoption of methodologies in acquiring evidence "live" from a suspect computer. Corrigan (2007) further notes that the collection order matters because volatile data changes over time. The order which the data should be acquired is network connections, ARP cache, login sessions, running processes, open files and the contents of RAM and other pertinent data. Evidence

collection is the single most important part of any digital forensics investigation (Rabin, 2010).

2.5.6 Digital Evidence Acquisition Methods

According to Garfinkel, (2010) in the laboratory, analysis performance follows the following steps: i) *Preventing contamination*: A copy of the original storage device is created before analysis of any digital evidence. The copy must be stored on another form of media to keep the original pristine. The destination storage unit should be new and if reused, it must be forensically “wiped” prior to use which will remove all the contents known and unknown existing in the media (Zdziarski, 2008). ii) *Isolate Wireless Devices*: isolation is usually done in the chamber to prevent connection to any networks and for the evidence to be perfect. Faraday bag can be opened inside the chamber and the device can be exploited, including phone information, Federal Communications Commission (FCC) information and SIM cards. If an agency does not have an isolation chamber, the researcher typically places the device in a Faraday bag and switches the phone to airplane mode to prevent reception (Lincke, 2015). iii) *Installing write-blocking software*: This prevents any changes to the data on the device or media. A block on the working copy should be installed to enable viewing only without changes or additions. iv) *Select extraction methods*: Once the working copy is created, the make and model of the device is determined and selecting extraction software designed to most completely “parse the data,” or view its contents. v) *Submit device or original media for traditional evidence examination*: When the data has been removed, the device is sent back into evidence. There may be DNA, fingerprint, trace or other evidence that might be obtained from it and the researcher can work without it. vi) *Proceed with investigation*: The selected software can be used to view data and also hidden data can be restored. Deleted files which normally are of value are also visible, as long as they have not been over-written by new data.

The researcher worked beyond the hardware to find evidence that resided on the internet including instant messaging, chat rooms, websites and other networks of participants or information. By using the system of Internet addresses, email header information, time stamps on messaging and other encrypted data, the researcher would be able to piece together strings of interactions that provide a picture of activity.

2.5.7 Digital Evidence Transportation

Ballou, (2010) states that digital evidence should not be kept in a vehicle for prolonged periods of time because the heat, cold or humidity can damage or destroy the evidence;

computers and electronic devices should be packed and secured to prevent damage from shock and vibration; also documentation of transportation should be done and maintenance of chain of custody on all evidence transported. Digital Evidence Storage should be stored in accordance with the agency's policies, in a secure climate-controlled environment that is not subject to extreme temperature or humidity. Digital evidence may be damaged or destroyed if exposed to magnetic fields, dust, and moisture or in vibration (Sullivan, Lynne & Terry, 2003).

2.6 Empirical Review

Adoptability of the technological models in courts will improve the trust and confidence by the public to the institution because of the access to justice and quality of justice offered (Chris, 2013). Digital forensic process model involves four steps; Acquisition, Identification, Evaluation and admission. There are new models that have been planned that will try and speed up the investigation processes and also solve various problems normally encountered in forensic investigation. Many leaders of the court don't focus well on IT issues; therefore they struggle hard to manage the technology projects.

According to Giles *et al.*, (2008), justices face no motivation in considering the preferences of the public any time the public is not in harmony with the Court. The outcomes of the court are normally influenced through variety of dynamics which include inter-branch conflict and public opinion Casillas (2011), shifting views and changing membership of the justices, and also the judicial norms and procedures.

Alexander Hamilton examined the Court as “an excellent barrier” besides “the oppressions and encroachments of the representative body” which served “as an important defence against the effects of the irregular ill humour in the society” (Hamilton, 1961). In this view, the Supreme Court protects justices from the public opinions. The relationship between Supreme Court and the public opinion come into view since justices' preferences will change with the reaction of the similar social forces that influence the public (Segal & Spaeth, 2002). IT governance as a formal structure tries to support technology tools by making decisions, resolving institutions problems, allocating the required resources and comes up with optimal solutions for the whole system and not for separate parts (Lawrence, 2012).

According to KEBANDE and RAY (2016), there are other existing models for digital forensics. Table 4 presents other existing models.

Table 4: A list of Digital Forensic Investigation Model.

Name of the model	Inventor and the year	Number of stages
Investigation process model	(Freiling & Schwittay, 2007)	4
Computer forensic field triage process model	(Roger <i>et al.</i> , 2006)	4
Investigation framework	(Kohn, Eloff, & Oliver, 2006)	3
Forensic process	(Kent <i>et al.</i> , 2006)	4
Event Based Digital Forensic Investigation Framework	(Carrier & Spafford, 2004)	16
Hierarchical, objective based framework	(Beebe & Clark, 2004)	6
Extended model of cybercrime investigation process	(Ciardhuain, 2004)	13
Enhance integrated digital investigation process	(Kelley & Knowles, 2016).	21
End to End digital investigation	(Stephenson, 2003)	9
An integrated digital investigation process	(Carrier & Spafford, 2003)	17
Abstract model of the digital forensic procedures	(Reith, Carr, & Gunsh, 2002)	9
Generic investigation process	(Al-Dhaqm <i>et al.</i> , 2016).	7
Computer forensic process	(Feng, Dawam & Amin, 2017).	4

Source: (Kebande & Ray, 2016)

2.6.1 An Abstract Digital Forensics Model (ADFM)

An Abstract Digital Forensics Model is an enhancement of the Digital Forensics Research Workshop (DFRW) investigative model since it is inspired from it (Reith, Carr & Gunsch, 2002). Figure 3 presents the abstract digital forensics model.

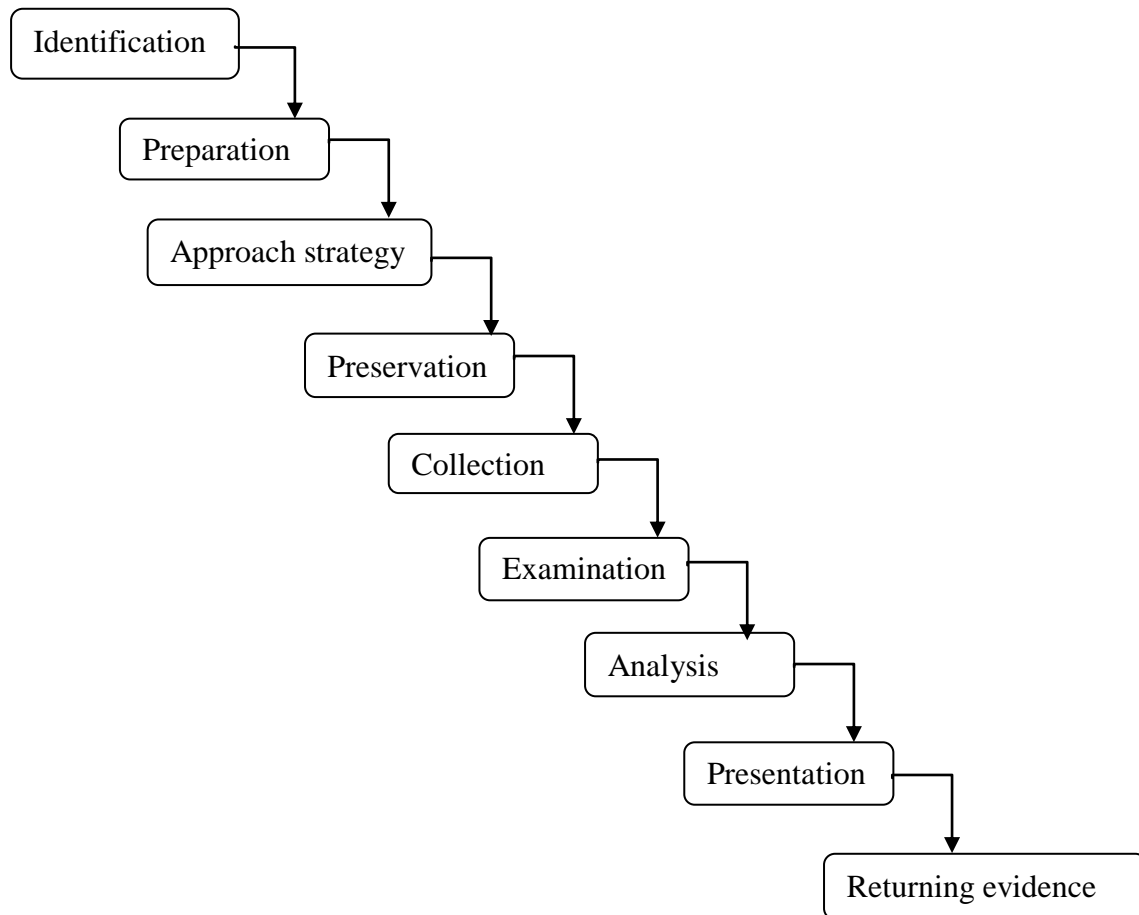


Figure 3: Abstract Digital Forensics Model.

(Source: Reith, Carr & Gunsch 2002).

In identification phase, the task and type of incident is performed; preparation is conducted and the approach strategy phase follows; isolation of the acquired physical and digital data is done, secured and also preserved which is under the preservation phase; data is then extracted and duplication is done under the collection phase; in examination phase, identification and locating of potential evidence follows; the analysis phase follows where determining of the significance of the evidence and drawing of conclusion based on the evidence found is done; Findings are then summarized and presented in the presentation phase; lastly returning of evidence phase winds.

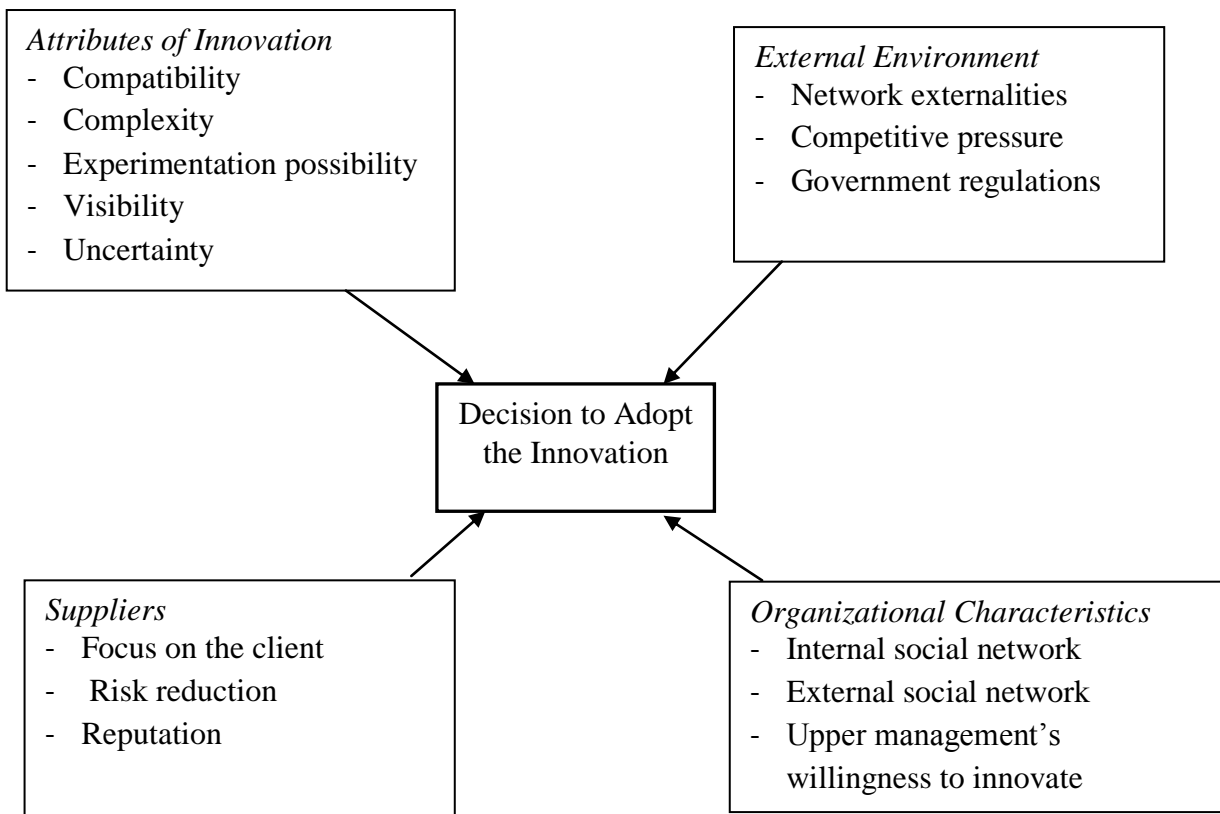


Figure 4: Technological Adoptability Model.

(Source: Lawrence, 2012)

2.7 Conceptual Framework

A conceptual framework is a product of qualitative process of theorization which interlinks concept that together provides a comprehensive understanding of a phenomenon or phenomena (Jabareen, 2009). The concepts that constitute this conceptual framework support one another, articulate their respective phenomena, and establish a framework-specific philosophy that defines relationships.

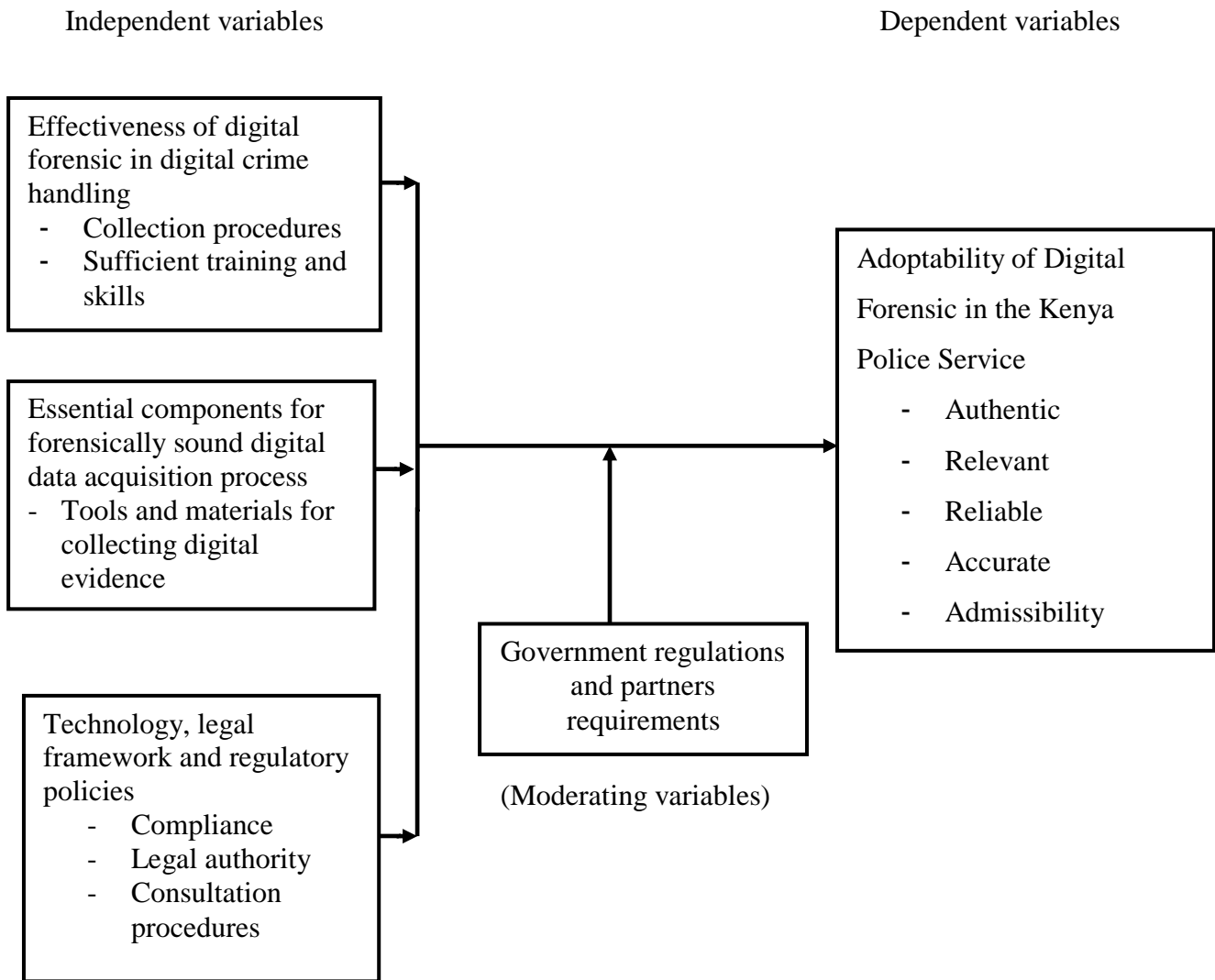


Figure 5: Conceptual Framework.

Independent variable is a variable that is supposed to determine a dependent variable. It can be changed and its values would not represent any problem requiring explanation in an analysis, but taken simply as specified (Pyrzczak, 2016). In this study the independent variables are; Effectiveness of digital forensic in digital crime handling; Essential components for forensically sound digital data acquisition process; and Technology, legal framework and regulatory policies. A dependent variable is that which is measured in the experiment and is affected during the experiment. The dependent variable responds to the independent variable (Everett, 2002). The dependent variable in this study was adoptability of digital forensic in the Kenya Police Service. The independent and dependent variables in Figure 5 have indicators which contribute one way or the other towards the variables within it. In case of changes in the government regulations (moderating variable), it can change the

independent variables directly or indirectly and as a result, adoptability of digital forensics which is the dependent variable will change accordingly.

2.8 Gaps in the Literature

From the literature, it is clear that there are various factors that directly affect digital evidence acquisition which are the major contributing factors to efficiency and effectiveness of cyber operations and the networks. There are several gaps in the current literature in relation to evidence acquisition that the researcher identified which include: collecting evidence from a static system, fully preservation of the state of the running system and the ruining of evidence by leaving footprints in the memory.

According to Quick (2014), “Digital evidence should be examined only by those trained specifically for that purpose.” With the wide variety of electronic devices in use today and the speed with which they change, keeping up can be very difficult for local law enforcement. Many agencies do not have a digital evidence expert on hand and if they do, the officer might be a specialist in cell phones but not social media or bank fraud. A detective may be able to log onto e-Bay and look for stolen property but may be unable to capture the device text message histories and could destroy evidence just by trying. Many take an interest in the area and learn what they can, but there is no single path to digital evidence expertise qualifications and certifications are not standardized across the country. The research addressed the gap by proposing a harmonized model that integrated technical and legal requirements to determine the admissibility of digital evidence in legal proceedings.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter presents the methods used in carrying out the research and the research design adopted by the study. It covers the tools, techniques and procedures used in the data collection. It also shows the target population, sample size and sampling technique used. This chapter concentrates more on the methods that were used in answering the research questions of the study.

3.2 Research Design

Research design refers to the general approach and framework chosen to incorporate the various components of the study in a comprehensible and rational way, ensuring the researcher successfully addresses the research problem. It comprises the outline for the collection, measurement, and analysis of data (Melyn, 2008).

This study employed a descriptive research design. The study adopted the cross sectional survey design as it was done within a short time, unlike the longitudinal survey design. A research design is the strategy for a study and the plan by which the strategy is to be carried out. It specifies the methods and procedures for the collection, measurement, and analysis of data. Descriptive research design was employed in collecting quantitative data. The study also employed a design science paradigm that was used in development of the model.

3.3 Location of the Study

The study was carried out in Nakuru County in Kenya.

3.4 Population of the Study

The target population was drawn from the Kenya Police Service in Nakuru County, Kenya, which is also part of the 47 counties in Kenya. This research targeted only on the Kenya Police from Nakuru county who dealt with forensics and had knowledge and skills in digital forensics.

3.5 Sampling procedures and Sampling size

This section discusses how the sample size was arrived at and the sampling used.

3.5.1 Sampling Procedure

A purposive sampling technique was used in the study in selecting of the sample. Purposive sampling aims at a particular group and a sample is not produced that is a representative of a larger population, though it can be closely what is required (Etikan *et al.*, 2016). This sampling design was used because the population of the study was expected not to be homogenous. After a pre visit by the researcher to the county, the following data was found and these made up the sample size. Table 5 shows the total number of respondents who had the knowledge and skills in digital forensics and makes up the target population.

Table 5: The Target Population.

Ranks	Target Population
Commissioner of Police (CP),	1
Senior Superintendent of Police (SSP),	1
Superintendent of Police (SP),	1
Assistant Superintendent of Police (ASP),	5
Chief Inspectors (CI),	5
Inspector (IP),	10
Senior sergeants (SSGT),	5
Sergeants (SGT),)	4
Corporals (CPL)	10
Police Constables (PC	10
Total	52

3.5.2 Sample Size

Cox (2018) says sample size depends on consideration of a number of factors including the quality of data, scope of the study, nature of topic, and also the study design used. Cox (2018) also makes an observation that the study that is broad in scope may require greater number of participants than one that is narrower in focus. Stratified sampling was used in categorization of respondents according to their ranks which formed the strata and purposive sampling because only respondents who had the desired characteristics in this case, knowledge on digital forensics were chosen. The sample size based on the above purposive sampling was 52 respondents.

3.6 Instrumentation

The questionnaires were used by the researcher to collect data. They were constructed based on the research objectives. The researcher preferred the questionnaires since they were easy to administer and time saving. The questionnaire contained closed-ended questions using liker scale (ranging from 1= No Extent; 2= Little Extent; 3= Moderate Extent; 4= Large Extent; 5=Very Large Extent). There were also a few open-ended questions which brought forth qualitative data on subjective thoughts and different responses related to access to digital evidence acquisition tools. Self-administered questionnaires were completed by those who could interpret the questionnaires. Some of the questions were administered by the researcher to respondents by use of interviews, for only those who did not have the ability to easily interpret the questions most likely because of their educational levels. Descriptive method was later used in analysis of the results.

3.7 Data Analysis

According to Terrizzano *et al.*, (2015), data obtained from the field in raw form is difficult to interpret unless it is cleaned, coded and analyzed. Qualitative analysis consists of examining, categorizing, tabulating and recombining evidences to address the research questions. Qualitative data was grouped into meaningful patterns and themes that were observed to help in the summarizing and organization of the data. Descriptive analysis was done using the Statistical Package for Social Sciences (SPSS).

3.8 Model Design and Implementation

3.8.1 Model Design

The equation used was expected to take a linear form as shown.

$$Y=C+\beta_1X_1+ \beta_2X_2+ \beta_3X_3+ \varepsilon$$

Where;

Y = Adoptability of digital forensic

C = Constant

$\beta_1, \beta_2, \beta_3, \dots, \beta_n$ = coefficients or the weights that were estimated.

ε = Standard error of estimate.

$X_1, X_2, X_3, \dots, X_n$ = variables; and in this study it is; Effectiveness of digital forensic, Technology legal framework and regulatory policies, components for forensic digital evidence and forensic adoptability model respectively.

3.8.2 Model Implementation

Implementation of the model was done by use of rapid prototyping. This was to obtain earlier feedback before creation of the final model. It assisted in testing and evaluation of the software and its workability. Rapid prototyping was chosen since it had the ability to develop customized products as per the individual's requirement and it required no special tools or process to implement design changes in the products.

3.9 Ethical Consideration

This is an important aspect in research where the researcher is expected to conduct the research with moral standards (Cooper, & Schindler, 2011). Respondents were free to take part in participation of the study. The researcher upheld ethical consideration during the research process and assured the respondents of confidentiality and that the information given was strictly to be used only for academic purpose. Attached see appendix VI, showing a letter of assurance of privacy and confidentiality of the information.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the analyzed data for the study. It begins with respondents' demographic information followed by the analysis based on the study objectives. It should be noted that 47 questionnaires were returned giving a response rate of 90%. This was seen to be appropriate to provide data.

4.2 Demographic Information

4.2.1 Gender

Table 6: Gender

Variable	Frequency (n)	Percentage (%)
Male	28	59.6
Female	19	40.4
Total	47	100.0

The finding showed that male respondents were 59.6% followed by females 40.4%. As observed, male respondents were more by 19.2% than the females.

4.2.2 Highest Academic Qualification

Table 7: Highest Academic Qualification

Variable	Frequency	Percentage %
Certificate	10	21.3
Diploma	14	29.8
Bachelor	20	42.6
Others	3	6.4
Total	47	100.0

It was discovered that bachelor and diploma holders were the majority with 42.6% and 29.8% respectively. Certificate holders were 21.3% and those in the category of 'others' were 6.4%.

4.2.3 A Cross tabulation of Gender and Length of Employment

Table 8: Cross tabulation of Gender and Length of Employment

Length of Employment	Males		Females	
	Count	% of total count	Count	% of total count
5 and below	12	25.5	8	17.0
6 - 10	11	23.4	11	23.4
11 - 20	2	4.3	0	0.0
21 and above	3	6.4	0	0.0
Totals	28	59.6%	19	40.4%

As displayed in Table 8, majority of male respondents had work experience of 5 years and below with 25.5% and 17% respectively, followed by 11% of both genders of who had worked for 6 to 10 years. Lastly, 21 years and above were only males with 6.4%.

4.2.4 Current Rank

Table 9: Current Rank

Variable	Frequency	Percent
Assistant superintendent	4	8.5
Chief Inspectors	5	10.6
Inspectors	9	19.1
Senior Sergeants	5	10.6
Sergeants	4	8.5
Corporals	10	21.3
Police Constables	10	21.3
Total	47	100.0

It was noted that the leading respondents were the Police Constables and Corporals with 21.3% followed by the Inspectors with 19.1%. Chief Inspectors and the Senior Sergeants were represented by 10.6% each while Assistant Superintendent and the Sergeants both had a representation of 8.5%.

4.2.5 Total Working Experience in the Field of Forensics

Table 10: Working Experience in the Field of Forensics

Variable	Frequency (n)	Percentage (%)
5 and below	12	25.5
6 – 10	34	72.3
11 – 20	1	2.1
Total	47	100.0

It was noted that 72.3% had worked for 6 – 10 years in the field of forensics. This implied that they were in a position to provide relevant data for the study. On the other hand, those who had worked below 5 years and 11-20 years were 25.5% and 2.1% respectively. As observed, the highest number of respondents with experience lied in between 6 – 10 years.

4.2.6 Familiarity to the Digital Forensics

Table 11: Familiarity to the Digital Forensics

Statement	No idea (%)	Not familiar (%)	Neutral (%)	Familiar (%)	Very Familiar (%)
Digital forensic policies and laws	21.3	0.0	40.4	0.0%	38.3
Digital forensic technologies	12.8	23.4	25.5	6.4	31.9
Digital forensics processes	23.4	40.4	10.6	4.3	21.3
Digital forensic evidence	10.6	53.2	27.7	2.1	6.4

It was renowned from the findings that regarding digital forensic policies and laws, 38.3% were very familiar while 21.3% had no idea. Similarly, 12.8% and 23.4% had no idea and unfamiliar with digital forensic technologies respectively. Digital forensics processes were very familiar to 25.6% while 63.8% were not. Finally, 63.8% were not familiar with digital forensic evidence.

4.3 Admissibility in Court of Law

Descriptive and quantitative analysis such as percentages were used to investigate patterns of variables under the study.

4.3.1 Effectiveness of Digital Forensic in Digital Crime Handling

Table 12: Effectiveness of Digital Forensic in Digital Crime Handling

Statement	SD	D	N	A	SA
Do you believe training and awareness is done regularly to improve on effectiveness of digital forensic services?	0.0%	6.4%	8.5%	29.8%	55.3%
Do you think the procedures & practices on digital forensic in avoiding inadmissibility of evidence are effective?	19.1%	25.5%	6.4%	14.9%	34.0%
Do you agree that all personnel performing digital forensics are effectively trained to perform their tasks?	10.6%	66.0%	8.5%	8.5%	6.4%
Do you think that the evidence collection procedures in your organization are effectively followed?	19.1%	61.7%	12.8%	4.3%	2.1%
Do you agree that effectiveness of digital forensic services in your organization improves on admissibility of evidence in court?	29.8%	53.2%	8.5%	4.3%	4.3%

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree

From the analyzed data, it was evident that 85.1% affirmed that training and awareness was done regularly to improve on effectiveness of digital forensic services. In addition, 83% disagreed that effectiveness of digital forensic services in their organizations improved on admissibility of evidence in court while 8.6% agreed that effectiveness of digital forensic services in their organizations improves on admissibility of evidence in court. Similarly, 44.6% disagreed that the procedures & practices on digital forensic in avoiding inadmissibility of evidence were effective while being supported by 76.6% who contended that all personnel performing digital forensics were not effectively trained to perform their tasks? Finally, only 6.4% affirmed that the evidence collection procedures in their organization were effectively followed leaving up to 80.8% having a contrary observation.

4.4 Technology, Legal Framework and Regulatory Policies

Table 13: Technology, Legal Framework and Regulatory Policies

Statement	SD	D	N	A	SA
The organization review its quality management system at least once every 3 years to ensure the system is meeting the quality needs of the organization	25.5%	46.8%	0.0%	14.9%	12.8%
The examiners do consult with the prosecutors or the organization’s counsel to resolve any questions about the authority to conduct a forensic examination	23.4%	23.4%	0.0%	36.2%	17.0%
The examiners do ensure they have the legal authority to search through the digital data they are examining	0.0%	27.7%	34.0%	19.1%	19.1%
The organization uses an outside entity to conduct digital forensics, and that the organization has taken documented steps to ensure the outside entity meets the standards outlined	10.7%	48.9%	40.4%	0.0%	0.0%
The technology we use do comply with legal requirements	17.0%	4.3%	0.0%	59.6%	19.1%

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree

It was seen that 27.7% maintained that the organization review its quality management system at least once every 3 years to ensure the system is meeting the quality needs of the organization. However, 72.3% differed. As to whether examiners do consult with the prosecutors or the organization’s counsel to resolve any questions about the authority to conduct a forensic examination, 46.8% disagrees with it. Moreover, 27.7% of respondents disagree that the examiners do ensure they have the legal authority to search through the digital data they are examining. It was clear that 59.6% reports that the organization does not use an outside entity to conduct digital forensics and that the organization has taken documented steps to ensure the outside entity meets the standards outlined. This observation could be further explained by lack of technology which complies with legal requirements 21.3% as asserted by responses.

4.5 Components for Forensic Digital Evidence.

Table 14: Components for Forensic Digital Evidence

Statement	SD	D	N	A	SA
I feel that there is need for other additional digital forensic tools to the institution	0.0%	6.4%	4.3%	12.8%	76.6%
We use tools that are thoroughly tested and acceptable legally	0.0%	0.0%	29.8%	53.2%	17.0%
I think digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions	25.5%	36.2%	19.1%	19.1%	0.0%
We have a well-established digital forensic lab with modem equipment/tools	14.9%	70.2%	2.1%	12.8%	0.0%
The institution ensures the tools they use to acquire digital evidence are validated to operate as intended and accurately acquire data	8.5%	53.2%	19.1%	19.1%	0.0%

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree

It was established that 89.4% declared that there was need for additional digital forensic tools to the institution. It was also affirmed by 70.2% respondents that they used tools that were thoroughly tested and acceptable legally. It was noted that 61.7% of respondents disagree that digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions as they lacked a well-established digital forensic lab with modem equipment and tools (85.1%). Only 19.1% agreed that the institution ensured that the tools they used to acquire digital evidence were validated to operate as intended and accurately acquire data.

4.6 Adoptability of Digital Forensic

Table 15: Adoptability of Digital Forensic

Statement	SD	D	N	A	SA
I consider digital forensic training as being relevant	0.0%	19.1%	0.0%	0.0%	80.9%
I consider digital evidence tools or components as being accurate	0.0%	0.0%	0.0%	40.4%	59.6%
There is more that is needed to improve on digital forensics processes to make the evidence more authentic	0.0%	19.1%	0.0%	21.3%	59.6%
I consider good governance on digital forensic ensures reliability in courts	0.0%	0.0%	0.0%	59.6%	40.4%
I consider good governance on digital forensic ensures admissibility in courts	0.0%	19.1%	0.0%	40.4%	40.4%

Key: SD = Strongly Disagree, D=Disagree, N = Neutral, SA = Strongly Agree, A = Agree

It was revealed that 80.9% agreed that they consider digital forensic training as being relevant. It was observed by all respondents (100%) that the digital evidence tools or components were accurate. It was observed that 80.9% of respondents affirmed that there is more that is needed to improve on digital forensics processes to make the evidence more authentic. This was clarified by all respondents who asserted that they consider good governance on digital forensic ensures reliability in courts. Finally, 80.8% reported that they consider good governance on digital forensic ensures admissibility in courts.

4.7 Model Derivation

This section presents spearman rho correlation analysis. This statistic was used to investigate whether there existed relationships between independent and dependent variables of the study. The findings are presented in Table 16.

Table 16: Correlation Analysis

		Adoptability of Digital Forensic	
Spearman's rho	Adoptability of digital forensic	Correlation Coefficient	1.000
		Sig. (2-tailed)	.
		N	47
	Effectiveness of digital forensic	Correlation Coefficient	.528**
		Sig. (2-tailed)	.000
		N	47
	Technology, Legal Framework and Regulatory Policies	Correlation Coefficient	.704**
		Sig. (2-tailed)	.000
		N	47
	Components for Forensic Digital Evidence.	Correlation Coefficient	.659**
		Sig. (2-tailed)	.000
		N	47

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

It was established that there exist a positive and statistically significant relationship between Adoptability of digital forensic and Effectiveness of digital forensic ($r=0.528^{**}$; $p<0.01$). This relationship is significant at 99 % confidence level (2-tailed). This means that sufficient training and skills coupled with good attitude towards digital forensic will positively affect adoptability of digital forensic. However, insufficient training and skills may hinder on adoptability of digital forensic services.

Additionally, it was recognized that there exist a positive and statistically significant relationship between adoptability of digital forensic and Technology, Legal Framework and Regulatory Policies ($r= 0.704^{**}$; $p<0.01$).The relationship is significant at 99% confidence level (2-tailed). This implies that the existing Technology, Legal Framework and Regulatory Policies affect positively Effectiveness of digital forensic services.

Furthermore, the finding revealed that there exist a positive and statistically significant relationship between Effectiveness of digital forensic and Components for Forensic Digital Evidence ($r= 0.659^{**}$; $p<0.01$). The relationship is significant at 99% confidence level (2-

tailed). This implies that the present components for forensic digital evidence affected positively Effectiveness of digital forensic services.

Finally, it was noted that there exist a positive and statistically significant relationship between Effectiveness of digital forensic and Forensic Adoptability ($r= 0.676^{**}$; $p<0.01$). The relationship is significant at 99% confidence level (2-tailed). This denotes that as the Forensic Adoptability improves it expands positively Effectiveness of digital forensic services.

4.8 Regression Analysis

Regression analysis is used to predict the influence of independent variables on dependent variable. The following Table 17 shows the model summary.

Table 17: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.819 ^a	0.670	0.647	0.369

a. Predictors: (Constant), Components for Forensic Digital Evidence., Effectiveness of digital forensic, Technology, Legal Framework and Regulatory Policies

From Table 17, it can be noted that 64.7% in the variation of adoptability of digital forensic can be expounded by the independent variables: Effectiveness of digital forensic, components for forensic digital evidence, Technology, Legal Framework and Regulatory Policies.

Table 18: ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.887	3	3.962	29.164	.000 ^b
	Residual	5.842	43	.136		
	Total	17.729	46			

a. Dependent Variable: Adoptability Model

b. Predictors: (Constant), Components for Forensic Digital Evidence., Effectiveness of digital forensic, Technology, Legal Framework and Regulatory Policies

These predictors are highly significant at 95% confidence level, $R^2=0.647$, $F=29.164$; $p<0.05$). In other words, the model is highly significant at 95% as shown in Table 18.

4.8.1. Regression Weights

The weights for the model that are illustrated in Table 19 were obtained from unstandardized beta coefficients.

Table 19: Coefficients^a

Model	Unstandardized Coefficients	
	B	Std. Error
(Constant)	0.528	0.364
Effectiveness of digital forensic	0.417	0.119
Technology, Legal Framework and Regulatory Policies	0.383	0.081
Components for Forensic Digital Evidence.	0.183	0.137

a. Dependent Variable: Adoptability Model

4.8.2. The Adoptability Model Equation

$$Y = C + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$$

$$\text{Adoptability of Digital Forensic} = 0.528 + (0.417 * \text{Effectiveness of digital forensic}) + (0.383 * \text{Technology, Legal Framework and Regulatory Policies}) + (0.183 * \text{Components for Forensic Digital Evidence}) + 0.369$$

4.9 Model Development

This section discusses how the model for determining the adoptability of digital forensics was determined.

4.9.1 Purpose of the Model

This research purposed to determine how effective the existing digital forensic collections tools were. In line with question four of this study, the model was implemented to provide an automated means of determining the adoptability of digital forensics as a web-based application.

4.9.2 System Functional Overview

The model was expected to allow user registration, logins, and forensic assessments. In addition, it was expected to take into consideration the respondents' inputs of forensic

assessments and to compute the adoptability thereof and where the adoptability fell below the thresholds, the model was to intelligently provide the necessary requirements for optimum adoptability.

a) Design Processes

Software Engineering and design processes were applied in the design of the model. In particular, the processes composed of the following activities:

- (i) Requirements Analysis:** All the system requirements were enumerated as expected deliverables then each of the requirement items was planned for. This process involved deciding best tools and technologies to use in order to deliver the best outcome as required. PHP scripting language, Open source Mysql database, CSS and JQuery were settled upon because they cost less to produce robust web-based applications.
- (ii) Specification:** All the specifications of the software system to be designed were outlined. This included how registration, login, assessments and reporting would be achieved.
- (iii) Software architecture:** The abstraction of the intended system was drawn showing how components would relate. This was to make certain that the software system would meet all the requirements.
- (iv) Implementation:** Rapid prototyping process was employed as the most ideal for designing the model. The database and tables were created and relationships defined. The processes were coded using PHP and JQuery and the output styled with CSS3
- (v) Evaluation:** After the design, the system was evaluated using objective-based or goal-based evaluation. This involved the designer testing of parts of software against the specifications. This was to make sure that codes for different components work together.

b) System Architecture

The software system architecture of the model involves many interrelated components, herein referred to as modules, that work together to achieve the main objective of the design and deliver specification details of the model. Several independent components compressed and running as PHP files were coded and Figure 6 presents how the independent components are interconnected.

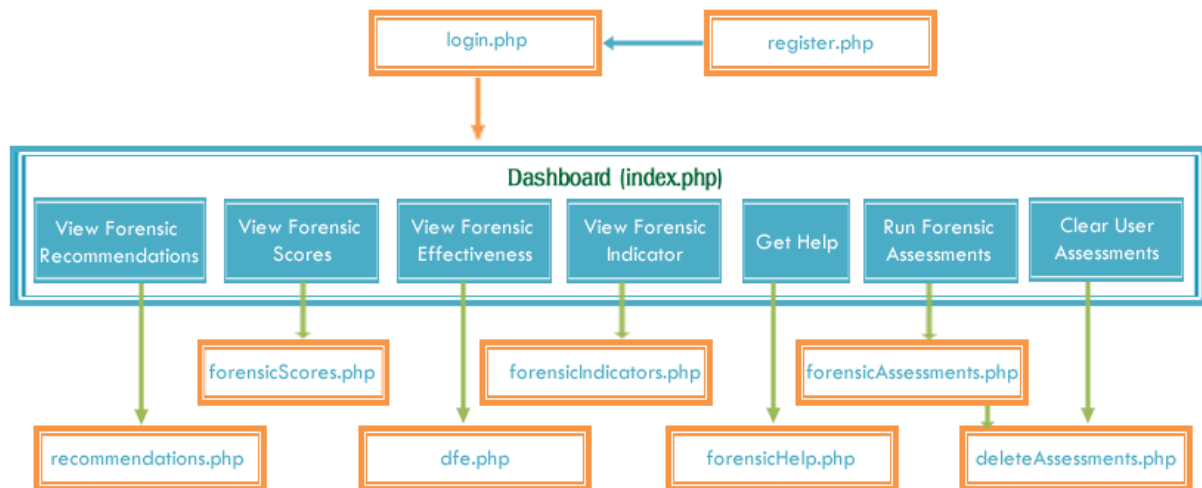


Figure 6: System Architecture

The summary of the specific independent components of the model are presented as follows;

- (i) **User Registration:** This acts as the starting point to using the model without which the subsequent system functions cannot be carried out. This module allows the user to register by providing their bio data information and then stores them in the database to be used later for authentication of users. This module applies SHA256 cryptography on all plaintext passwords provided by the user before they are stored in the database.
- (ii) **User Login:** This is the entry point to the system for registered users. It authenticates registered users, sets up user sessions.
- (iii) **User Logout:** This is the exit point of the system for registered users. It destroys user sessions when they click logout button or when they stay idle for long.
- (iv) **User Navigation:** This allows the users to navigate through the system easily and load different pages easily depending on the activities they intent the carry out within the system. There are two types of menu that assure easy navigation within the system; namely, the header menu and footer menu.
- (v) **User Dashboard:** This component provides the user with a quick view of their adoptability status by providing vital information about; their percentage forensic adoptability, their performance as regards various forensic adoptability indicators, their average forensic scores, the number of times they have run forensic assessments and the number recommendation they have.
- (vi) **Forensic Assessments:** This presents the user with forensic statements for which they assess in a Likert scale of 1 to 5 and submit results, herein referred to as forensic scores,

to the database. Forensic scores form this component forms the basis for computing adoptability and generating other vital outputs.

(vii) **Help Module:** This component provides guidelines to the user on how to carry out several varied functionalities of the system.

(viii) **User Reports:** This component provides vital reports to the user once they are done running forensic assessments. The reports produced by this component include; forensic scores report, forensic recommendations report and forensic evaluation of adoptability report available to the admin.

(ix) **Databases:** The model is driven by MySQL relational database engine with three database tables, namely users, forensic_assessments and forensic_questions.

4.9.3 Software Engineering and Design

Software engineering and design of the model was achieved using PHP programming language for controls, MySQL database engine for storing system data, JQuery and JavaScript to add response to the system and CSS3 to style the layout of the model. This section presents how different components of the model for determining the adoptability of digital forensics were developed.

a) Registration Module

For a respondent to get entry to the platform and perform assessment for forensic adoptability of their digital forensics evidence collection tools, they are required to register. This process entails submitting details to the system that will be used to gain entry on subsequent logins. Such information includes; the name of the user, their email address, Institution, username and their strong password. Dully filled registration form can be submitted. In this case, PHP scripts to fetch user posts and inserts them into the database. This module is enriched with form validation tools, for instance, the email provided during registration must meet the email format criterion, and the passwords provided must be strong enough. At the database level this module assures privacy of user passwords by ensuring that no plain text (readable) passwords are stored in the database. It is therefore responsible for encryption and storage of encrypted passwords. On the overall, the registration module serves as the point of entry to the platform. Figures 7 and 8 are a presentation of the registration module flow chart and system interface respectively;

Register to Digital Forensics System

I agree With Terms and Conditions

OR

Figure 7: User Registration Form

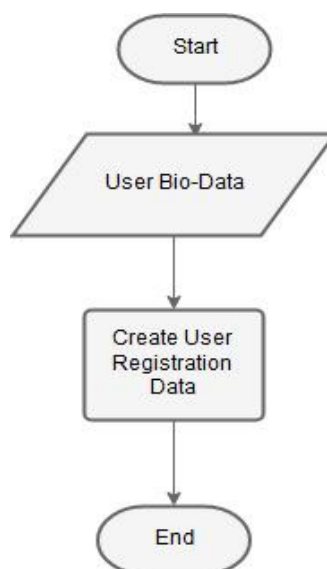


Figure 8: Registration Flowchart

b) Login Module

The login module of the model controls access to the system by ensuring that only registered and authorized users can proceed with other system functions. This therefore implies that the user must be registered and must provide the correct email and password in order to be

allowed to access the platform's home page. Besides, this module is responsible for the management of user sessions whereby sessions are setup once the users successfully logs into the system and sessions are destroyed when they logout.

Basically the login module queries the user database and allows access if and only if the email provided by the user can be located in the database and the password provided matches the decrypted value of the corresponding password. If the user email cannot be located in the users' database, the system displays an error message that the user with the inputted email does not exist. Similarly, if the password does not match the decrypted value of the corresponding password, then the system display an error message that the password provided is incorrect. In either of this cases the system loops back to the login module as presented in the Figures 9 and 10 as flowchart and graphical user interface respectively.

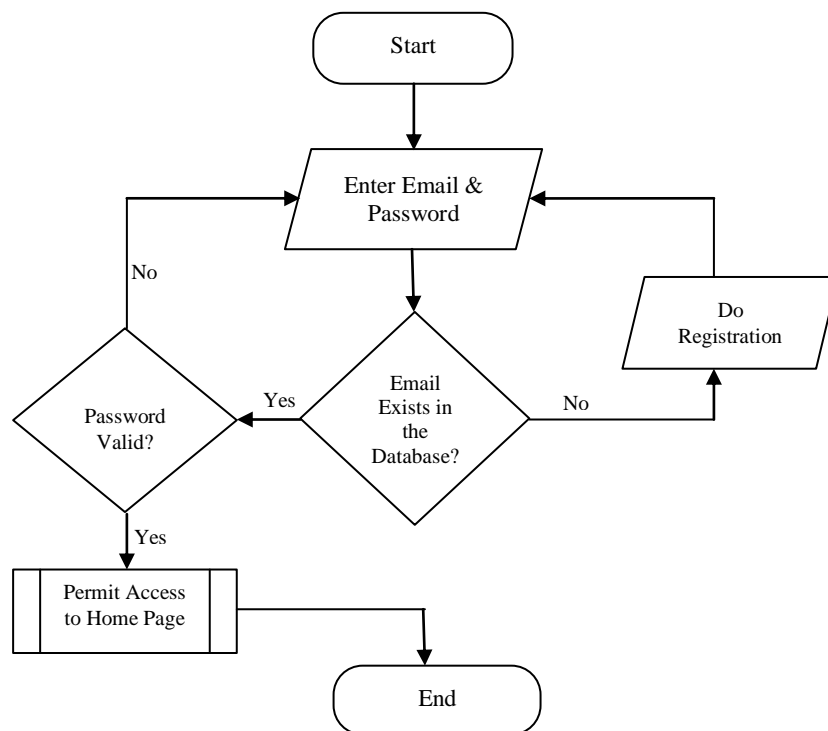
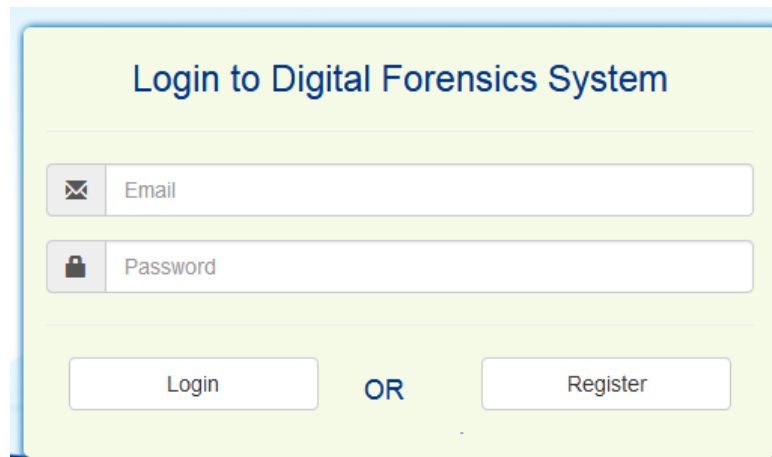


Figure 9: Login Flowchart



The image shows a login form titled "Login to Digital Forensics System". It features two input fields: "Email" with an envelope icon and "Password" with a lock icon. Below the fields are two buttons: "Login" and "Register", separated by the text "OR".

Figure 10: Login Form

c) Dashboard

A successful login leads the user to the homepage herein referred to as dashboard. At the dashboard, the user is able to have a quick view of their digital forensic assessment statistics if they have active assessments. This includes the overall percentage index pointing to their adoptability as regards to digital forensics evidence collection tools. If there is no record of active assessments for the user, then the display on the dashboard informs the user that there are no active assessments denoted by 0. Figure 11 shows a system dashboard for a new user who has no active assessments whereas Figure 12 portrays a dashboard for a user who has done proceeded to do forensic assessment. Still at the dashboard, users with active assessments can know the number of recommendations of actions required for optimum adoptability as well as the average score of all the assessment scores based on the all active assessments belonging to the logged in user.

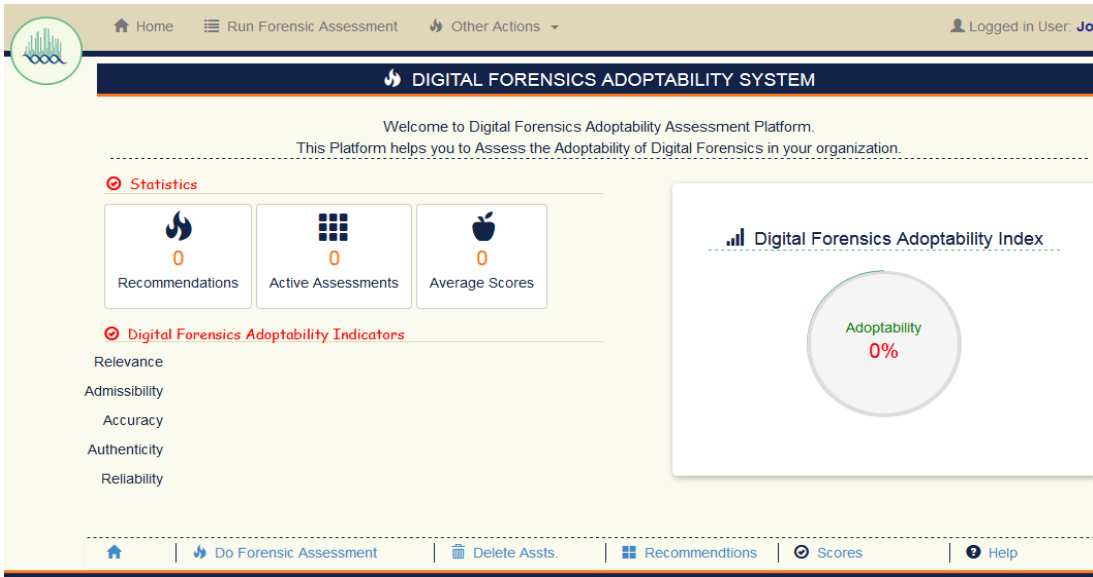


Figure 11: Dashboard with no Active Assessments for the Logged in User

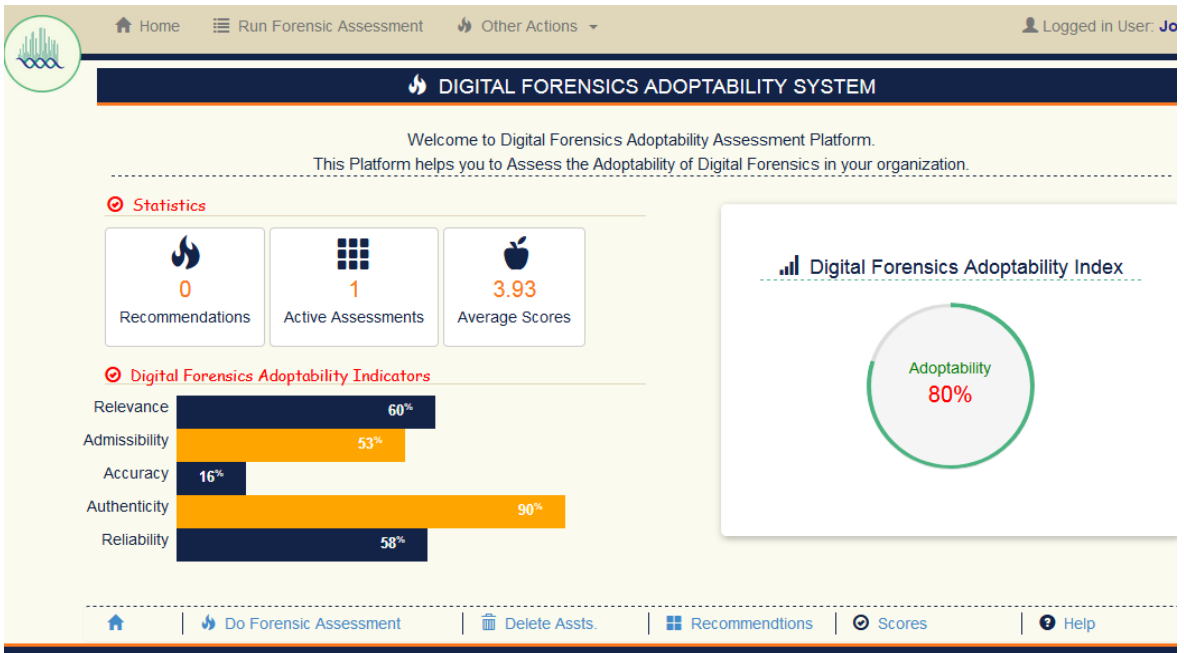


Figure 12: Dashboard with One Active Assessment for the Logged in User

d) System Navigation

The system allows the users to navigate easily within the system. Menu techniques were used to assure easy navigation. Two menu panels were used in the model; namely, the header menu as shown in Figure 13 and footer menu as presented in Figure 14.

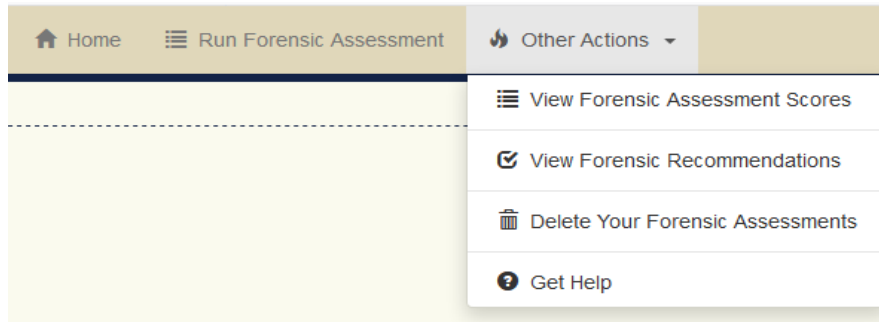


Figure 13: Header Menu.

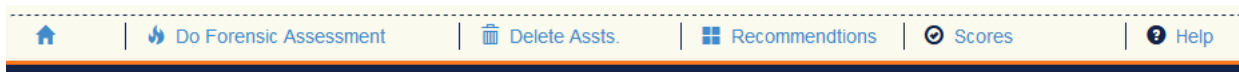


Figure 14: Footer Menu.

e) Digital Forensic Assessment Module

This module enables the users of the platform to carry out the main purpose for which this model was developed, that is, to perform digital forensic assessments. The results of the exercise carried out in this module are scores which are very significant in determining the adoptability of digital forensics in the user’s institution. To achieve this, the module extracts the forensic assessment questions from the database using PHP scripts and presents them to the user in a readable and well organized manner using Cascaded Style Sheets version 3 (CSS3). Additionally, using HTML5 and CSS3, the assessment options for the user for each forensic assessment question is presented in form of a Likert scale between 1 and 5 where; 1 represents Strong disagreement to corresponding statements while 5 represent Strong agreement to the statements.

The digital forensics assessment module also allows the users to choose the most appropriate responses to each forensic assessment statements and to submit their dully-filled form to the database. Behind the scenes, the module inserts the user responses into MYSQL database engine using PHP scripts where they are stored to be used later in computing the adoptability of digital forensics. The graphical user presentation of the digital forensics assessment module is presented in Figure 15 while the flowchart presentation of the forensic assessment process is presented in Figure 16.

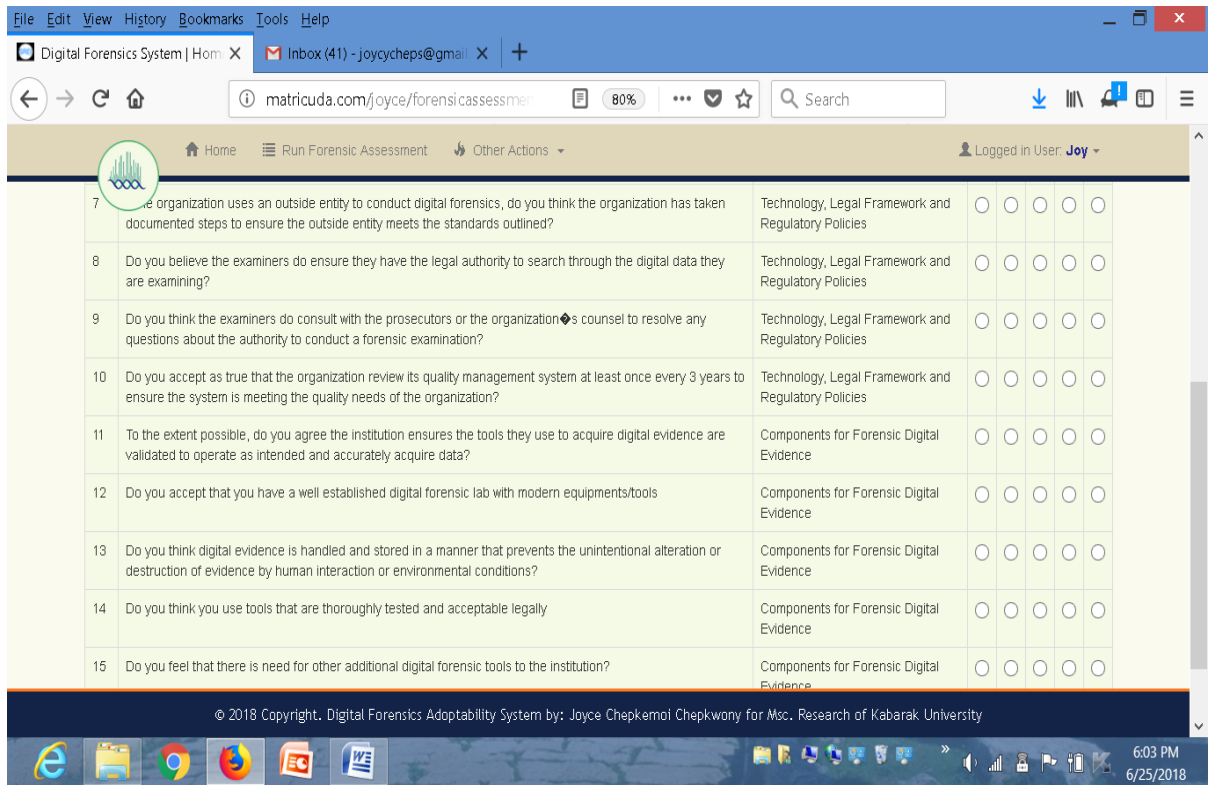


Figure 15: Forensic Assessments Page

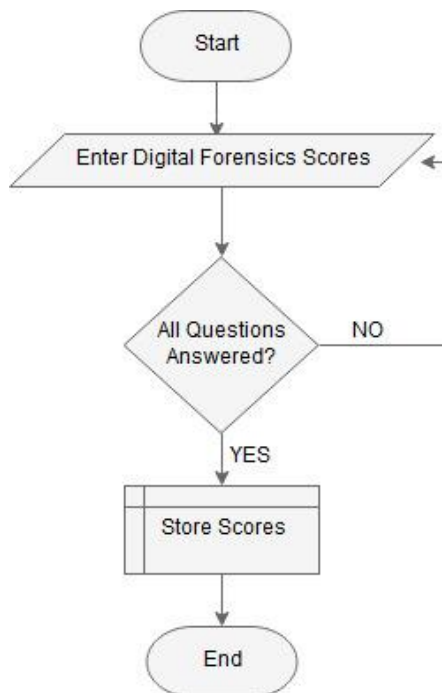


Figure 16: Adoptability of Digital Forensics Flowchart

f) Adoptability Index Gauge

The formula derived after regression analysis in section 4.8.2 was implemented in the model basically to compute the adoptability of digital forensic. This factored in the all the scores belonging to the logged in user to compute the adoptability. The formula was automated as a PHP code as presented in the snippet in Figure 17. A more interactive and readable presentation of the adoptability outcome for the user was done using web tool namely, HTML5 to publish the Gauge, CSS3 for styling and JavaScript to animate the output. Figure 17 show the digital forensics adoptability output based on assessment scores for the active user.

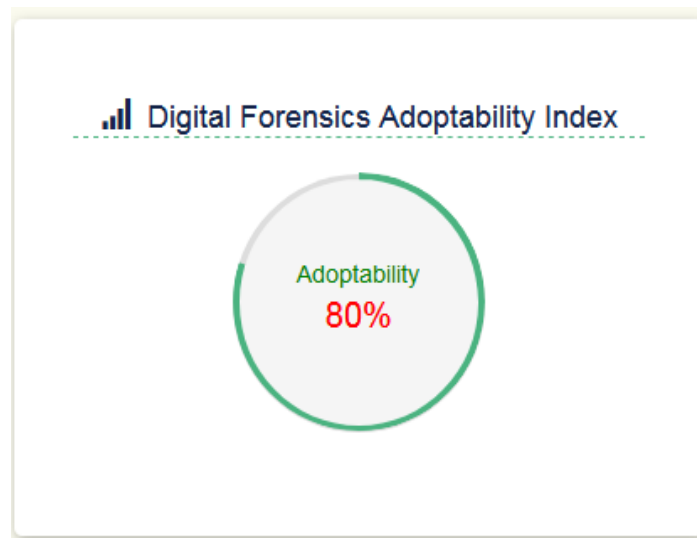


Figure 17. Forensic Adoptability Index Gauge

g) Adoptability Indicators

This is a section of the dashboard display that gives the user a quick view of adoptability of the digital forensics with respect to five forensics indicators; namely, Admissibility, Relevance, Authenticity, Accuracy and Reliability. The adoptability is computed for each indicator independently as percentage index and a comparative display of all the five indicators is presented as a responsive horizontal bar graph. This helps the users and their organizations to know the level of adoptability of their digital forensic collection tools with regard to the five indicators. The presentation of the comparative graph of digital adoptability of forensic tools in relation to the five indicators is shown in Figure 18.

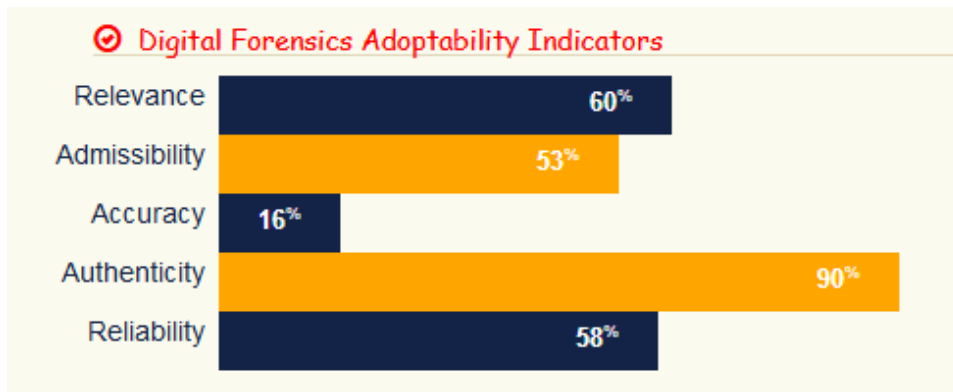


Figure 18: Forensic Adoptability Indicators

h) Adoptability Index Calibration

Based on the formula that was derived and used in the model to automate determination of digital forensics adoptability, auspicious observations were made in regards to the output of model. The upper limit of the scale is index 1 or 100 percent. This is achieved when the user checks all the forensic assessment questions with score 5; meaning, they strongly agree to all the assessment statements. The lower limit, on the other hand, was observed to be index 0.23 or 23 percent. This is possible when the user disagrees strongly to all forensic assessment statements by scoring 1 for all the questions. The model as an instrument can possibly measure adoptability of digital forensics between indices 0.23 and 1 or, put in other words, 23 percent to 100 percent. This is referred to as a possible case.

The user, however, cannot achieve adoptability of between 0 and 23% simply because the choice of scale for this research was a scale 1 to 5 Likert. The fact that the adoptability indices below 0.23 cannot be achieved, it can be explained simply with two reasons; one, the scale cannot allow the users to post score 0 during forensic assessment, and two, the constant and the error term in the derived equation cannot permit outright 0 adoptability. The adoptability below index 0.23 in this case is referred to as the impossible case. Figure 19 presents the calibration of the model as an instrument while equation 2 shows the PHP code snippet of the equation that was used to compute adoptability of digital forensics.

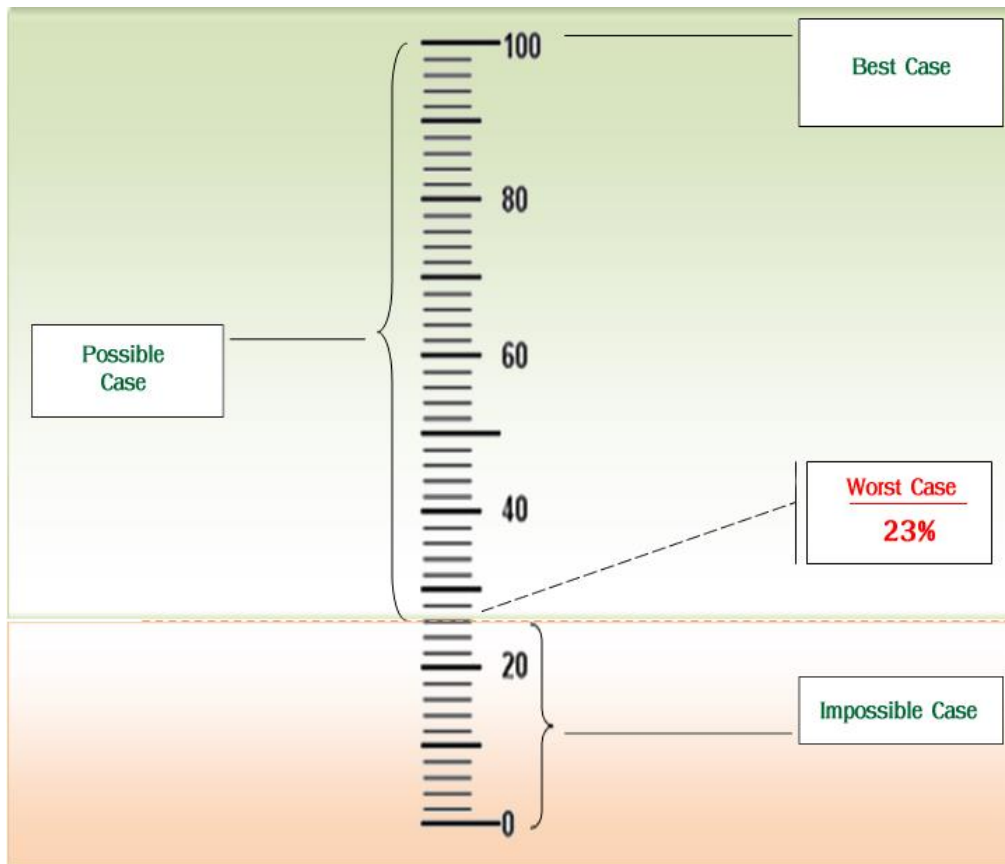


Figure 19: Model Cases

```
$adoptability = "SELECT ROUND (((0.528+SUM (a.forensicscore * b.categoryweight) + 0.369) / (0.528+SUM (5 * b.categoryweight) + 0.369)*100), 0) FROM forensicassessments a INNER JOIN forensicquestions b ON a.questionid=b.id INNER JOIN users c ON a.userid=c.id WHERE a.userid=$user_id;";
```

i) Other Statistics

The statistics panel was available at the user dashboard. This helped the user to have a quick info of their average scores. The mean score was basically the average of all the range of user forensic scores in a scale of 1 to 5. Where the user had some scores below the threshold, then the statistics panel enumerates to the user the number of requirements needed to achieve best case of adoptability of digital forensic tools. Finally, the statistics panel informed the user on whether they had previous active assessments for them to choose whether to clear them and carry out a fresh forensic assessment or proceed with another forensic assessment to get the average of all the assessments. The Figure 20 presents the statistics panel that provided vital information to the user.

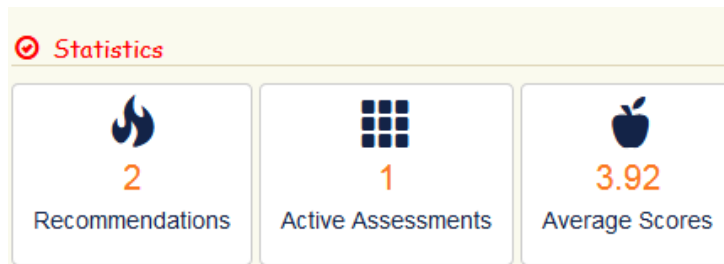


Figure 20: Statistics Panel

j) Forensic Scores

This component was designed to capture the forensic assessment scores that are stored in the database and output them back to the user. This was seen as vital to allow users to revisit their previous assessments and preview how they had awarded scores to various forensic statements. The module was programmed to filter the scores of the logged in user without accessing or interfering with the other users' records. The users can only see their own results of assessments which are enumerated and grouped by the dates when the forensic assessments were carried out. This module allows the user to view the scores for all their forensic assessments irrespective of the number of times the logged in user did forensic assessments. The user therefore can read through the scores in HTML format or print or download the scores in portable document format (pdf). The process of how the module is able to retrieve the scores from the database is shown in Figure 21 as a flowchart. Figure 22 presents the HTML output of the module while Figure 23 presents forensic scores in a printable and portable format.

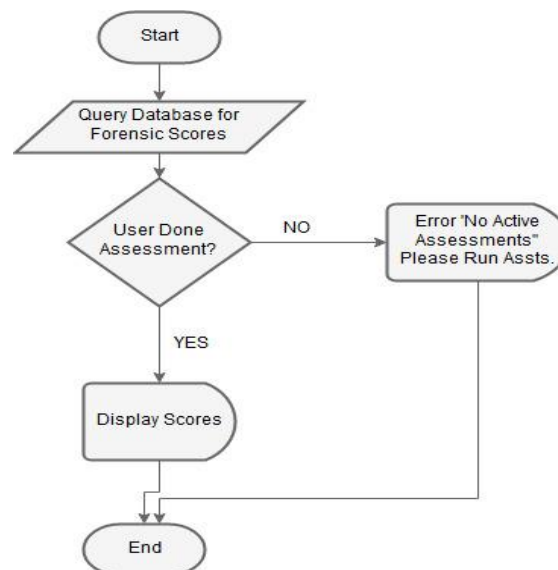


Figure 21: Forensic Score Flowchart

No.	Date of Assessment	Forensic Question	YourInput
1	2018-06-08 12:31:34	Do you agree that all personnel performing digital forensics attend to a formal training program for the tasks they perform?	1
2	2018-06-08 12:31:34	Do you believe training and awareness is done regularly on digital forensic services and processes?	2
3	2018-06-08 12:31:34	Do you agree the institution screens digital forensic applicants to ensure they possess the highest standards of conduct and ethics, including unimpeachable honesty and integrity?	3
4	2018-06-08 12:31:34	Do you agree the forensic personnel pass a practical proficiency test at least once every 3 years?	4
5	2018-06-08 12:31:34	Do you consider good governance on digital forensic ensures reliability and admissibility in courts?	4

Figure 22. Forensic Scores in HTML Output

Question Id	Assessment Date	Forensic Score
1	2018-06-07 10:29:26	1
2	2018-06-07 10:29:26	2
3	2018-06-07 10:29:26	3
4	2018-06-07 10:29:26	4
5	2018-06-07 10:29:27	3
6	2018-06-07 10:29:27	3
7	2018-06-07 10:29:27	4
8	2018-06-07 10:29:27	5
9	2018-06-07 10:29:27	5
10	2018-06-07 10:29:27	4

Figure 23: Forensic Scores in PDF Output

k) Forensic Recommendations Module

This module, like the scores module, is a results-display module whose output is based on logged-in user's active forensic assessments. As shown in Figure 24, the system checks if the logged-in user has done forensic assessments and scores are stored in the database. If there are no such records, then the system prompts the user to run fresh forensic assessment and submit forensic score to the database. The system, otherwise filters database forensic scores belonging to the logged-in user and compare them with the corresponding threshold scores. If the scores are below the threshold scores, then the system outputs them as requirements necessary to attain optimum adoptability. The output is initially in HTML format but the user is provided with a leeway to download or print the forensic recommendations in pdf format. Figures 25 and 26 presents HTML and PDF outputs of the forensic recommendation module respectively.

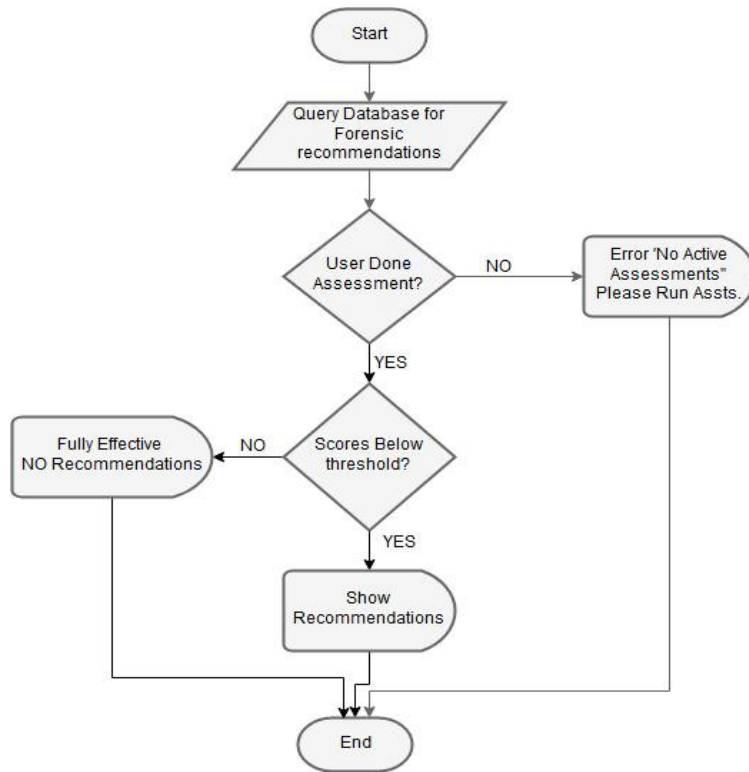


Figure 24: Forensic Recommendations Flowchart.

Forensic Recommendations			
No.	Forensic Recommendation	YourInput	Indicators
1	All personnel performing digital forensics should attend to a formal training program.	1	People
2	Training and awareness should be done regularly on digital forensic services and processes	2	People

Figure 25: Forensic Recommendation HTML.

FORENSIC RECOMMENDATIONS PDF		
QuestionId	Score	Forensic Recommendations
1	1	All personnel performing digital forensics should attend to a formal training program for the tasks they perform.
2	2	Training and awareness should be done regularly on digital forensic services and processes

Figure 26: Forensic Recommendation PDF

1) Forensic Help Module

Although the model was designed with the latest web technologies to achieve easy-to-read and interactive platform, it is prudent to guide the user on how to carry out the activities once

logged in successfully. This module therefore provides guidelines to the user on how to do forensic assessments, how to delete previous assessments in case the user wishes to, how to get forensic recommendations from the system, how to check user scores, and most importantly, how to interpret the forensic adoptability from the output of the model. This module was designed as accordion collapsible panels with help topics as panel headings that can be read by the users easily. The details are collapsed within the inner panels to spare the users from lengthy, tiresome and rather unnecessary literature. The help panel is presented in Figure 27 as accordion collapsible panels.

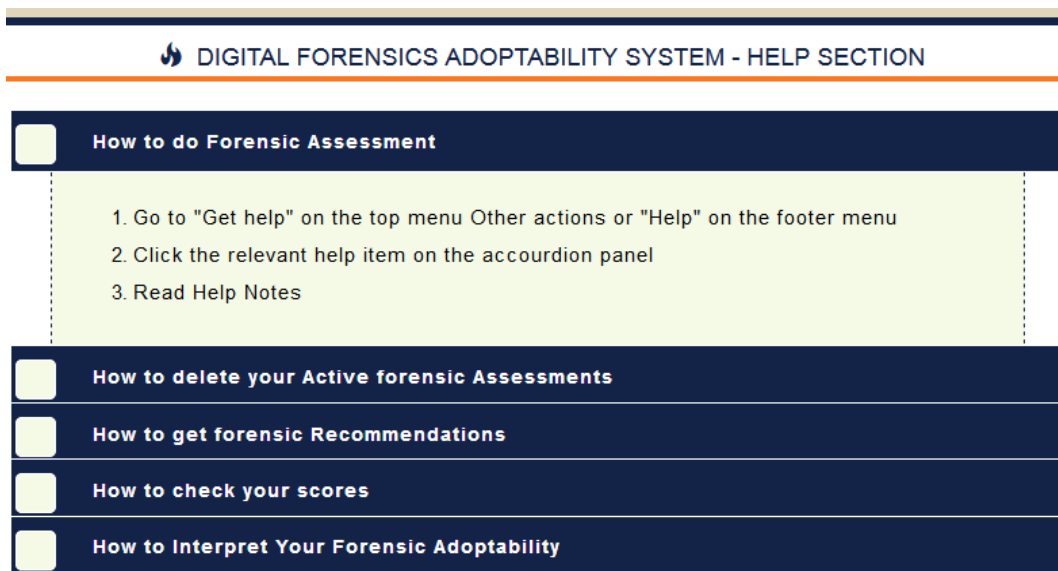


Figure 27: Forensic Help Module

m) Entity Relationship Diagram

Three primary database tables were used to store the model data; namely, forensicassessments, forensicquestions and users table. The forensicquestions table stores all the forensic statements required in forensic assessments. It also stores, thresholds below which the system retrieves recommendations, category, category weights, indicators and corresponding recommendations. Users table, on the other hand, stores user details including user id, user names, organization and password hashed with SHA256 hashing algorithm. Lastly, the forensicassessments table stores assessment id which is an auto-increment field, associated question id, user id, forensic score and the date of assessment.

The forensicassessments and forensicquestions tables share a many-to-many relationship where the many assessment questions for which the users award scores equally submits an array of forensic scores to forensicassessments table. Similarly, user and forensicassessments

tables share a one-to-many relationship. This implies that one user posts an array of forensic scores to the forensicassessments table. Figure 28 presents an entity relationship diagram for the Digital forensic acquisition system.

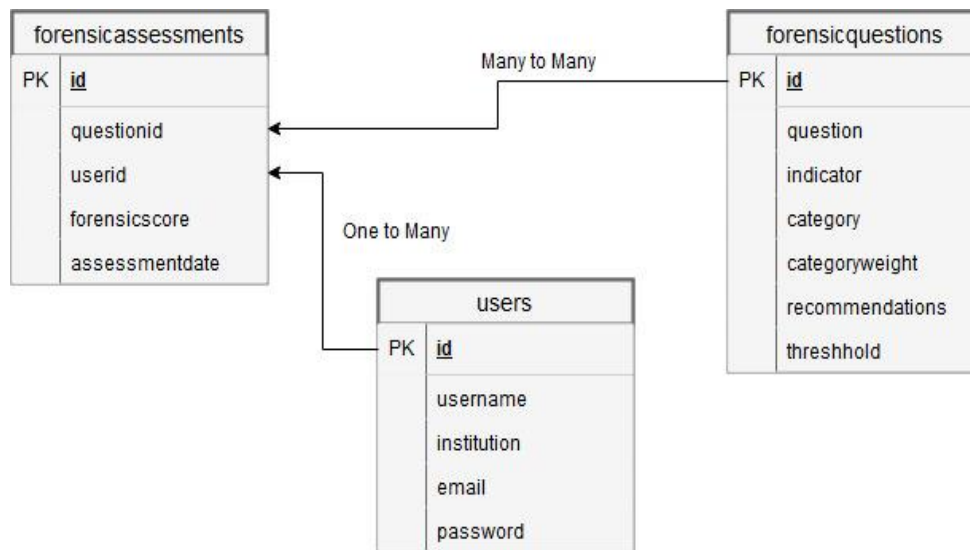


Figure 28: Entity Relationship Diagram

n) Proof of Concept

As a proof of concept, the digital forensics acquisition model was designed as a web-based application using latest web tools. MySQL database was used to store records that drive the model; namely, forensic users, forensic assessment statements, recommendations and forensic assessment scores for the users. Hypertext Preprocessor (PHP) was used as a server-side language to insert and retrieve data into and from the database. JQuery and Javascript were used to animate the model and add interaction to it, particularly on the output panels. Finally, the layouts were styled using Cascaded Style Sheets version 3 (CSS3). The model was designed on Cross-Platform Apache, MySQL, PHP and Perl (XAMPP) as a local server and PHPStorm as a local code editor. The complete web-based model was deployed to a public web server where it can be accessed remotely though the following URL; www.matricuda.com/joyce

4.10 Evaluation of the Model

The model was evaluated after the design process to ascertain that it could perform the intended purposes. The intended objectives were set prior to design process and used for evaluation as deliverables checklist when the design was done. As presented in Table 20, the delivered outcomes are tabulated alongside the intended goals. All the set objectives were achieved as shown in Table 20. To sum it up, the system performed well intended functions.

Table 20: Model Evaluation

Components	Goals	Delivered Outcomes
Registration	<ol style="list-style-type: none"> 1. Accept user Bio-Data 2. Post User Data to the Users Database 3. Hash Passwords at the Database Level 	<ol style="list-style-type: none"> 1. User Registration Form Accepts User Bio-data. 2. User Data Successfully posting to MySQL Database. 3. Passwords Hashed using SHA256
Login	<ol style="list-style-type: none"> 1. Permit Login with Correct email and password 2. Redirect user to Dashboard upon successful login 	<ol style="list-style-type: none"> 1. System Permits Login with Correct email and password 2. System Successfully redirects the users to their corresponding Dashboards upon successful login
Navigation	<ol style="list-style-type: none"> 1. Allow easy Navigation within the model 	<ol style="list-style-type: none"> 1. Easy navigation using two menus; that is, top menu and footer menu. 2. Dashboard panels provide links to various other pages
Dashboard	<ol style="list-style-type: none"> 1. Display digital forensic adoptability 2. Display forensic adoptability indicators 3. Display quick statistics 	<ol style="list-style-type: none"> 1. Digital forensic adoptability display achieved as an interactive percentage gauge. 2. Five forensic adoptability indicators display achieved through interactive horizontal bar graphs 3. Quick statistics panels for average forensic scores, active assessments and forensic recommendations
Forensic Assessments	<ol style="list-style-type: none"> 1. Retrieve Questions from database 2. Present 1 to 5 Likert scale to users for each question 3. Post the forensic scores to the database 	<ol style="list-style-type: none"> 1. Model retrieves forensic questions from database 2. Likert scale presentation achieved through use of five radio buttons for each forensic assessment question 3. Forensic scores can be posted to the database.
Forensic Scores	<ol style="list-style-type: none"> 1. Forensic Scores to be retrieved after assessment 2. Scores to be Portable 	<ol style="list-style-type: none"> 1. System retrieves Scores for the logged-in user 2. Scores can be exported to PDF
Forensic Recommendations	<ol style="list-style-type: none"> 1. Recommendations to be retrieved after assessment 2. Recommendations to be Portable 	<ol style="list-style-type: none"> 1. System retrieves recommendations for the logged-in user 2. Recommendations can be exported to PDF
Security	<ol style="list-style-type: none"> 1. System to be secure 	<ol style="list-style-type: none"> 2. System require login to proceed. 3. Passwords are hashed using SHA256. 4. Sessions are quickly destroyed when idle 5. Confidentiality assured because users are limited to view results from their own assessments.

Besides the designer’s model evaluation, the model remote URL was sent out to as many users as possible to verify the model by registering users, logging in and performing forensic assessments which was the primary purpose of the model. After several days, the results were checked to ascertain that the users registered, logged in and ran forensic assessment successfully as expected. The Figure 29 presents the output of successful forensic assessments for various users. To strictly preserve ethical standards of anonymity, users’ institutions and their emails could not be displayed.

DIGITAL FORENSICS ADOPTABILITY SYSTEM		
Assesseees and their Adoptability Scores		
Name of the Assessee	Date of Forensic Assessment	Adoptability of Digital Forensics(%)
Joshua	2018-06-25 21:47:41	70
Joy	2018-07-23 14:28:35	84
Irene	2018-06-04 15:56:21	66
ibu	2018-06-05 13:02:40	76
David	2018-06-15 08:29:34	88
Sheila	2018-06-15 11:32:57	80
sheila	2018-07-23 14:53:07	89
marylyne	2018-08-03 15:06:13	72
john	2018-09-11 13:08:09	85

Figure 29. User Verification – Professional Analysis

4.11 Security of the Model

The design of the model factored in the main information security tenets, namely Confidentiality, Integrity and Authenticity (CIA). Confidentiality was assured using secure authentication and session setup. Only registered users could login and view records related to them. Integrity was also preserved by ensuring that users could only manipulate their own records and could not change other users’ records. For instance, a user could delete only their previous forensic assessment scores and no one else’s. Ultimately, availability was assured by ensuring that the applications were hosted online with web hosts with least down-time records. Users could therefore access the system and carry out system functions anytime they wished to.

4.12 Areas of Further Improvement

Although this model was designed using best web technologies to achieve a web-based application, further improvement can be done to it by giving it a new dimension. A mobile application would be ideal in this case because of the fast emerging mobile technologies and ease of use.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the conclusions of the study by giving summary of how the study questions were answered. In addition, the recommendations and further studies are also presented in this chapter.

5.2 Conclusions

The study aimed at investigating the adoptability of digital forensics in digital crime handling in Kenya police service that would assist to achieve high digital security level parameters and lessen the existing problems. The study developed a user-friendly and easy-to-use web-based model to determine the adoptability of digital forensics in the institutions of study. The following sections 5.2.1 to 5.2.4 presents how each of the study questions was answered.

5.2.1 Research Question 1: How can Digital Forensics in Digital Crime Handling in Kenya Police Service be Effective?

The study established that the institutions conducted trainings and awareness sessions regularly to improve on effectiveness of digital forensic services. Even though responses indicated a still low level of effectiveness regarding digital forensic services necessary to improve the admissibility of evidence in court. The study further found out that the procedures & practices on digital forensic for avoiding inadmissibility of evidence were still basically accessioned by the fact that the evidence collection procedures in their organization were effectively followed.

5.2.2 Research Question 2: How will Technology, Legal Framework, Regulatory Policies and Practices Contribute towards Admissibility of Digital Forensics?

It was established from the study that a greater percentage of respondents agreed that the technology they used in their institutions complied with legal requirements, however little review was being done to ensure that the system they used met quality needs of their organizations. Therefore, this address to technologies affected admissibility of digital forensics evidence in courts. As to whether legal framework contributed towards admissibility of digital forensics, respondents agreed that there were legal frameworks that allowed them to search through the digital data. This was facilitated by the consultation they

had with the prosecutors or organisational counsels regarding questions about the authority to conduct forensic examinations, hence, legal framework contributes towards admissibility of digital forensics. Jin (2017) notes that, further complications of the research will continue to evolve as long as there is still rapid advancement of technologies, the increased globalization of the virtual environment and the reactive nature of the countries regulatory processes, the field will continue to mature.

5.2.3 Research Question 3: What are the Outcomes of the Examination of the Essential Components that Make up Forensically Sound Digital Data Acquisition Process?

The study further established that, although digital forensic tools existed in the institutions under study, respondents felt a dire need for additional digital forensic tools. Besides the fact that the tools were thoroughly tested and legally accepted, many do not think that the digital evidence are handled and stored in a manner that stops alterations and destruction. The study portrayed that the institutions lacked well-established digital forensic labs with modern equipment and tools and that they do not validate tools for acquisition of digital forensic evidence to ensure they operate as intended. In today's digital world, it has become very important for any criminal investigator, to have in mind that the use of tools and technical skills alone is not enough to fully investigate any digital crime. A well-defined process should be followed that goes beyond just the technical needs (Nelson, 2008).

5.2.4 Research Question 4: How will the Adoptability Model be developed?

As described in chapter four, the model for determining the adoptability of digital forensics in organization was designed as a web based application using the latest web technologies. Precisely, PHP server – side scripting language was used to program the system controls, CSS3 was used for system styling, MySQL was used as a database engine. The model was hosted as an online platform where users could register, login and access the system functions remotely via the URL link that was widely communicated. The system was verified to have succeeded in performing all the intended functions, namely; user registration, user login, forensic assessment, computation of adoptability index and production of relevant reports.

5.3 Recommendations

The study noted that the collection and handling of digital evidence by the police in Kenya could be improved if best practices could be employed. This study therefore highlighted the following key recommendations to improve the admissibility of the evidence in courts;

5.3.1 Training and Awareness

The study noted good trends of training and awareness matters (85.1%) in the police service as regards digital forensics. However, the research recommends that more training and awareness exercises, done regularly, would be necessary to further improve efficiency of service delivery by the forensic personnel within the police. This will help the officers to handle digital forensic matters even as the attacks on the cyber space continue to intensify while digital crimes continue to be reported.

5.3.2 Recommendations for further research

ICT is dynamic and new issues keep emerging. In lieu of this, digital forensic evidence acquisition and handling tools and components need to be reviewed and improved regularly. The research therefore recommends that more funding to digital forensics departments of the Kenya Police would be necessary if admissibility of digital evidence in courts was to be improved.

REFERENCES

- Adams, R. (2013). *"The emergence of cloud storage and the need for a new digital forensic process model"* (PDF). Murdoch University.
- Al-Dhaqm, A., Razak, S. A., Othman, S. H., Nagdi, A., & Ali, A. (2016). A generic database forensic investigation process model. *Jurnal Teknologi*, 78(6-11), 45-57.
- Ballou, S. (Ed.). (2010). *Electronic crime scene investigation: A guide for first responders*. Diane Publishing.
- Beaney, M. (2012). Analysis. *The Stanford Encyclopaedia of Philosophy*. Retrieved 23 May
- Becker, R. F. (2005). *Criminal investigation*. Jones & Bartlett Learning
- Caelli, W. J., & Liu, V. (2018). Cyber security education at formal university level: An Australian perspective. In *Journal for the Colloquium for Information Systems Security Education*. 5(2): 26-44. CISSE.
- Card, S. K. (2017). *The psychology of human-computer interaction*. CRC Press.
- Carrier, B. & Winter (2003). *Defining Digital Forensic examination and analysis Tools Using Abstraction layers*. International Journal of Digital Evidence.
- Carrier, B., & Spafford, E. H. (2003). *Getting physical with the digital investigation process*. International Journal of digital evidence, 2(2), 1-20.
- Carrier, B., (2004). *Digital Forensic Research Workshop*. dfrws.org
- Casey, E. (2007). *What does "forensically sound" really mean? Digital Investigation*.
- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Academic press
- Casey, E., & Turnbull, B. (2011). *Digital evidence on mobile devices*. Forensic Science, Computers, and the Internet, Third Edition. Academic Pres.
- Casillas J., Enns P K., & Wohlfarth P. C (2011). *How public opinion constrains the US Supreme Court*. American Journal of Political Science; 55(1):74–88.
- Checkland, P., & Poulter, J. (2006). *Learning for Action: A Short Definitive Account of Soft Systems Methodology and its Use for Practitioners, Teachers and Students*. Chichester: John Wiley.
- Chike, C. P. (2016). *Impediments of Effective Incident Response and Handling in a Medium Sized Information Technology Organization* (Doctoral dissertation, Capitol Technology University).
- Cole, G. F., Smith, C. E., & DeJong, C. (2018). *The American system of criminal justice*. Cengage Learning.
- Conrad, C. (2010, October 3). *Cell phones cause hang-up for police to track drug deals*. Mail

- Cooper, D.T., & Schindler, P.S. (2011). *Business Research Methods*. Mumbai: Tata
- Corrigan, R. (2007). *Digital Decision Making*. Springer-Verlag London Limited.
- Ćosić, J., & Bača, M. (2010). A framework to (im) prove chain of custody in digital investigation process. In *Proceedings of the 21st Central European Conference on Information and Intelligent Systems (CECIIS)* (pp. 43-438).
- Cox, D. R. (2018). *Applied statistics-principles and examples*. Routledge.
- Crouch, J. E. (2012). *An introduction to computer forensics*. NSCI; [http://www.nsci-va.org/WhitePapers/2010-12-16-Computer% 20Forensics-Crouch-final.pdf](http://www.nsci-va.org/WhitePapers/2010-12-16-Computer%20Forensics-Crouch-final.pdf).
- Cummins Flory, T. A. (2016). Digital forensics in law enforcement: A needs based analysis of Indiana agencies. *Journal of Digital Forensics, Security and Law*, 11(1), 4.
- Drucker, P. (2017). *The age of discontinuity: Guidelines to our changing society*. Routledge.
- Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, 9, S90-S98.
- Eales, N. (2016). Risk assessment. *Missing Persons: A Handbook of Research*, 160.
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4.
- Fallows, J. (2008). The connection has been reset. *Atlantic Monthly*, 301(2), 19.
- Feng, X., Dawam, E. S., & Amin, S. (2017). Digital forensics model of smart city automated vehicles challenges.
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, 86, 13-23.
- Fisher, B. A., & Fisher, D. R. (2012). *Techniques of Crime Scene Investigation*. crc Press
- Fraser, J. (2017). Making Domestic Violence a Crime: Situating the Criminal Justice Response in Canada. In *Global Responses to Domestic Violence* (pp. 41-59). Springer, Cham.
- Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital investigation*, 7, S64-S73.
- Giles, M. W., Bethany B., & Richard L. (2008). The Supreme Court in American Democracy: *Unravelling the Linkages between Public Opinion and Judicial Decision Making*. *Journal of Politics* 70(2): 293–306.

- Grobler, C. P., Louwrens, C. P., & von Solms, S.H. (2010) A multi-component view of digital forensics. In *Availability, Reliability, and Security, 2010 ARES'10 International Conference on* (pp.647-652).
- Guarino, A. (2013). Digital forensics as a big data challenge. In *ISSE 2013 securing electronic business processes* (pp. 197-203). Springer Vieweg, Wiesbaden.
- Gupta, J. N., Kalaimannan, E., & Yoo, S. M. (2016). A heuristic for maximizing investigation effectiveness of digital forensic cases involving multiple investigators. *Computers & Operations Research*, 69, 1-9.
- Hannan, M., Frings, S., Broucek, V., & Turner, P. (2003). *Forensic computing theory and practice: towards developing a methodology for a standardised approach to computer misuse* (Doctoral dissertation, Edith Cowan University).
- Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information Systems*, 47, 98-115.
- Hope, K. R. (2018). The police corruption “crime problem” in Kenya. *Security Journal*, 1-17.
- Hossain, M., Hasan, R., & Skjellum, A. (2017). Securing the internet of things: a meta-study of challenges, and open problems. In *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)* (pp. 220-225). IEEE.
- Howard Jr, J. W. (2014). *Courts of appeals in the federal judicial system: A study of the second, fifth, and District of Columbia circuits*. Princeton University Press.
- Jansen, W., & Grance, T. (2011). Sp 800-144. *Guidelines on security and privacy in public cloud computing*.
- Jin, D. Y. (2017). *Smartland Korea: Mobile communication, culture, and society*. University of Michigan Press.
- Jones, A. (2008, January 21–23). Keynote speech. In: *First International Conference on Forensic*
- Jones, R. 2008. *Safer Live Forensic Acquisition*. University of Kent at Canterbury. Available from: <http://www.cs.kent.ac.uk/pubs/ug/2007/co620-projects/forensic/report.pdf>
- Kadish, S. H., Schulhofer, S. J., & Barkow, R. E. (2016). *Criminal law and its processes: Cases and materials*. Wolters Kluwer Law & Business.
- Kaur, R., Saini, K., & Sood, N. C. (2013). Application of video spectral comparator (absorption spectra) for establishing the chronological order of intersecting printed strokes and writing pen strokes. *Science & Justice*, 53(2), 212-219.
- Kebande, V. R., & Ray, I. (2016, August). A generic digital forensic investigation framework for internet of things (iot). In *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on* (pp. 356-362). IEEE

- Kelley, T. R., & Knowles, J. G. (2016). A conceptual framework for integrated STEM education. *International Journal of STEM Education*, 3(1), 11.
- Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security*. Jones & Bartlett Publishers.
- Kshetri, N. (2013). *Cybercrime and cyber security in the global south*. Springer.
- Lawrence, P. (2012). *The NCSC court IT Governance model*.
- Lessing, M., & Von Solms, B. (2008). *Live forensic acquisition as alternative to traditional forensic processes*.
- Lubaale, E. C. (2015) & Bokolo, V. S. (2014): The practicality of challenging DNA evidence in court. *South African Crime Quarterly*, 52(1), 39-47.
- Lutui, R. (2016). A Multidisciplinary digital forensic investigation process model. *Business Horizons*, 59 (6), 593-604
- Manish, L. (2013). *Cyber Law: A Global Perspective*.
- Moreau, D. M. (2013) "*Fundamental Principles and Theory of Crime Scene Photography*" Quantico: Forensic Science Training Unit, FBI Academy.
- Moturi, C. A. (2011). *Digital forensics framework for Kenyan courts of laws* (Doctoral dissertation, University of Nairobi).
- Mrdovic, S., Huseinovi A., & Zajko, E., (2009). *Combining Static and Live Digital Forensic Analysis in Virtual Environment*.
- Murphy, G. (2015). *Cellular Phone Evidence Data Extraction and Documentation*. (PDF).
- National Crime Agency, (2016). *Need for a stronger law enforcement and business partnership to fight cyber crime*
- National Research Council. (2009). *Strengthening forensic science in the United States: a path forward*. National Academies Press.
- Nelson, B., et al., (2008). *Computer-forensics-investigation-case-study*. Infosec Institute.com
- Nelson, B., Phillips, A., & Steuart, C. (2014). *Guide to computer forensics and investigations*. Cengage Learning.
- Nikkel, B. J. (2006). *Improving evidence acquisition from live network sources*. *Digital investigation*, 3(2), 89-96.
- Oriwoh, E., & Williams, G. (2015). Internet of Things: The argument for smart forensics. In *Handbook of research on digital crime, cyberspace security, and information assurance* (pp. 407-423). IGI Global.

- Overill, R., & Chow, K. P. (2018). Measuring Evidential Weight in Digital Forensic Investigations. In *IFIP International Conference on Digital Forensics* (pp. 3-10). Springer, Cham.
- Peltier, T.R. (2013). *Information Security Fundamentals*. CRC Press.
- Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation, 13*, 38-57.
- Pyrczak, F. (2016). *Making sense of statistics: A conceptual overview*. Routledge.
- Quick, D., & Choo, K. K. R. (2014). Data reduction and data mining framework for digital forensic evidence: storage, intelligence, review and archive.
- Rabin, S. (2010). *Computer Evidence*. Cengage Learning.
- Rafique, M., & Khan, M. N. A. (2013). Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific & Engineering Research, 4*(10), 1048-1056.
- Rahman, S., & Khan, M. N. A. (2015). Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology, 8*(2), 379-88.
- Reith, M., Carr C.; Gunsch, G (2002). *An examination of digital forensic models*. *International Journal of Digital Evidence*. Archived from the original on 15 October 2012. Retrieved 2 August 2010.
- Robertson, B., Vignaux, G. A., & Berger, C. E. (2016). *Interpreting evidence: evaluating forensic science in the courtroom*.
- Sahai, A., & Waters, B. (2014). How to use indistinguishability obfuscation: deniable encryption, and more. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*
- Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209.
- Simon, R. (2009). Policy Brief Nr 16, October 2009: *Addressing the challenges of law enforcement in Africa*. Policing in Sierra Leone, Tanzania and Zambia.
- Skoog, D. A., Holler, F. J., & Crouch, S. R. (2017). *Principles of instrumental analysis*. Cengage learning.
- Slay, J., Hannan, M., Broucek, V. & Turner, P. (2004). "Developing forensic computing tools and techniques within a holistic framework: an Australian approach," *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop*, pp. 394-400.

- Soltani, S., & Seno, S. A. H. (2017). A survey on digital evidence collection and analysis. In *Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on* (pp. 247-253). IEEE.
- Soltani, S., & Seno, S. A. H. (2017, October). A survey on digital evidence collection and analysis. In *Computer and Knowledge Engineering (ICCKE), 2017 7th International Conference on* (pp. 247-253). IEEE.
- Sullivan, L. P., & Childs, S. T. (2003). *Curating archaeological collections: from the field to the repository* (Vol. 6). Rowman Altamira.
- Tajuddin, T. B., & Manaf, A. A (2015). Forensic investigation and analysis on digital evidence discovery through physical acquisition on smart phone. In *Internet Security (WorldCIS), 2015 World Congress on*, pp.132-138. IEEE, 2015.
- Taveras, P. (2013). SCADA live forensics: real time data acquisition process to detect, prevent or evaluate critical situations. *European Scientific Journal, ESJ*, 9(21).
- Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.
- Terrizzano, I. G., Schwarz, P. M., Roth, M., & Colino, J. E. (2015, January). Data Wrangling: The Challenging Journey from the Wild to the Lake. In *CIDR*.
- Throup, D. (2017). Crime, politics and the police in colonial Kenya, 1939–63. In *Policing and decolonisation*. Manchester University Press.
- Tyler, T. R., & Jackson, J. (2014). Popular legitimacy and the exercise of legal authority: Motivating compliance, cooperation, and engagement. *Psychology, public policy, and law*, 20(1), 78.
- Walsh, S. J. (2018). Australasian forensic science summit 2016: the external future context and the case for change. *Australian Journal of Forensic Sciences*, 50(3), 245-258.
- Wayne, J., & Ayers, R. (May 2007). *Guidelines on cell phone forensics*. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>
- Weedon, J., Nuland, W., & Stamos, A. (2017). Information operations and Facebook. *Version, 1*, 27.
- Wilding, E. (2017). *Information risk and security: preventing and investigating workplace computer crime*. Routledge.
- Xynos, K., Harries, S., Sutherland, I., Davies, G., & Blyth, A. (2010). Xbox 360: A digital forensic investigation of the hard disk drive. *Digital Investigation*, 6(3-4), 104-111.
- Zdziarski, J. (2008). *iPhone forensics: Recovering evidence, personal data, and corporate assets*. "O'Reilly Media, Inc."
- Zhang, Y., Wu, J., Zukerman, M., & Yung, E. K. N. (2015). Energy-efficient base-stations sleep-mode techniques in green cellular networks: A survey. *IEEE communications surveys & tutorials*, 17(2), 803-826.

APPENDIX I: Letter of Introduction

Joyce C. Chepkemoi
P.O. Box 1910,
Nakuru.
Tel No.: 0720 259766

28th January 2018

TO WHOM IT MAY CONCERN

Dear Sir / Madam,

RE: PERMISSION TO CARRY OUT ACADEMIC RESEARCH

I am a Master of Science in Information Technology Security and Audit student at Kabarak University, Nakuru conducting a research study on ‘Adoptability model for digital forensic evidence in Kenya’. The reason for this letter is to request for permission to carry out the research study in your institution which is part of the university requirement for a master’s degree. This will entail filling in of questionnaires and any information given will be treated with utmost confidentiality and will only be used for the purpose of research.

Thanks in advanced.

Yours faithfully,

JOYCE .C.CHEPKEMOI

	1	2	3	4	5
Digital forensic evidence					
Digital forensics processes					
Digital forensic technologies					
Digital forensic policies and laws					

PART B: Effectiveness of digital forensic in digital crime handling

In the scale of 1 to 5, please tick the most appropriate answer to the questions in relation to the above. (**KEY: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree**)

	1	2	3	4	5
1. Do you believe training and awareness is done regularly to improve on effectiveness of digital forensic services?					
2. Do you think the procedures & practices on digital forensic in avoiding inadmissibility of evidence are effective					
3. Do you agree that all personnel performing digital forensics are effectively trained to perform their tasks?					
4. Do you think that the evidence collection procedures in your organization is effectively followed?					
5. Do you agree that effectiveness of digital forensic services in your organization improves on admissibility of evidence in court?					

6. What do you think the technical understanding of the prosecutors presenting digital evidence at hearings and at trials affect the effectiveness of that evidence to the fact-finder?

PART C: Technology, Legal Framework and Regulatory Policies

In the scale of 1 to 5, please tick the most appropriate answer to the questions in relation to digital forensics (**KEYS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree**)

	1	2	3	4	5
1. Do you consider the technology you use do comply with legal requirements					
2. If the organization uses an outside entity to conduct digital forensics, do you think the organization has taken documented steps to ensure the outside entity meets the standards outlined?					
3. Do you believe the examiners do ensure they have the legal authority to search through the digital data they are examining?					
4. Do you think the examiners do consult with the prosecutors or the organization’s counsel to resolve any questions about the authority to conduct a forensic examination?					
5. Do you accept as true that the organization review its quality management system at least once every 3 years to ensure the system is meeting the quality needs of the organization?					

6. How do the courts rule when faced with challenges on admissibility of digital forensics?

PART D: Components for Forensic Digital Evidence.

In the scale of 1 to 5, please tick the most appropriate answer to the questions in relation to digital forensics (**KEYS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree**)

	1	2	3	4	5
1. To the extent possible, do you agree the institution ensures the tools they use to acquire digital evidence are validated to operate as intended and accurately acquire data?					
2. Do you accept that you have a well established digital forensic lab with modern equipments/tools					
3. Do you think digital evidence is handled and stored in a manner that prevents the unintentional alteration or destruction of evidence by human interaction or environmental conditions?					
4. Do you think you use tools that are thoroughly tested and acceptable legally					
5. Do you feel that there is need for other additional digital forensic tools to the institution?					

Part E: Adoptability of digital forensic

In the scale of 1 to 5, please tick the most appropriate answer to the questions in relation to digital forensics evidence.

(**KEYS: 1=strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree**).

	1	2	3	4	5
1. In your own opinion, do you consider good governance on digital forensic ensures admissibility in courts?					
2. In your own opinion, do you consider good governance on digital forensic ensures reliability in courts?					

3. Do you think that there is more that is needed to improve on digital forensics processes to make the evidence more authentic?					
4. Do you agree that the digital evidence tools or components as being accurate?					
5. In your own opinion, do you consider digital forensic training as being relevant?					

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

Thanks for your time.

APPENDIX III: System Code

System Login

```
<?php
ob_start();
session_start();
require_once 'dbconnect.php';

// if session is set direct to index
if (isset($_SESSION['user'])) {
    header("Location: index.php");
    exit;
}

if (isset($_POST['btn-login'])) {
    $email = $_POST['email'];
    $upass = $_POST['pass'];

    $password = hash('sha256', $upass); // password hashing using SHA256
    $stmt = $conn->prepare("SELECT id, username, password FROM users WHERE email=
?");
    $stmt->bind_param("s", $email);
    /* execute query */
    $stmt->execute();
    //get result
    $res = $stmt->get_result();
    $stmt->close();

    $row = mysqli_fetch_array($res, MYSQLI_ASSOC);

    $count = $res->num_rows;
    if ($count == 1 && $row['password'] == $password) {
        $_SESSION['user'] = $row['id'];
        header("Location: index.php");
    } elseif ($count == 1) {
        $errMSG = "Bad password";
    } else $errMSG = "User not found";
}
?>
```

Forensic Assessment

```
<?php
ob_start();
session_start();
require_once 'dbconnect.php';

if (!isset($_SESSION['user'])) {
    header("Location: login.php");
```



```

    exit;
}
// select logged in users detail
$res = $conn->query("SELECT * FROM users WHERE id=" . $_SESSION['user']);
$userRow = mysqli_fetch_array($res, MYSQLI_ASSOC);

?>
<!DOCTYPE html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <title>Digital Forensics System | Home</title>
    <link rel="stylesheet" href="assets/css/bootstrap.min.css" type="text/css"/>
    <link rel="stylesheet" href="assets/css/index.css" type="text/css"/>
</head>
<body style="background-image:url('assets/images/bg2.jpg');">

    <div class="container">
        <div class="row">
            <br><br><br>
        </div>
        <div class="row" style="text-align:center;">
            <h4 style="border-bottom:1px dashed
#132347;color:#132347;padding-bottom:3px;"><span class="glyphicon glyphicon-folder-
open">&nbsp; Digital Forensics Adoptability Model - Forensic Assessment
Section</h4>
            <p style="background:#132347; color:#ffffff;padding:5px;border-
bottom:3px solid #FB7820">In the scale of 1 to 5, please tick the most appropriate answer to
the questions in relation
                Adoptability of Digital Forensics. <br>(KEY: 1=strongly disagree,
2=Disagree, 3=Neutral, 4=Agree, 5=strongly Agree)</p>
            </div>
            <div class="row">
                <?php include 'topmenu.php';?>
                <form action="" method="post" >
                    <?php
                        include_once 'dbconnect.php';
                        $sql = "SELECT category,id,question FROM
forensicquestions;";
                        $result = mysqli_query($conn,$sql);
                        $json = array();
                        if (mysqli_num_rows($result) > 0) {
                            echo "<table class='table table-bordered table
table-hover table-sm' style='background: #F5FAE6;'>
                                <tr style='color:#002F3F;'>
                                    <th>NO</th>
                                    <th>Questions</th>
                                    <th>Category</th>
                                    <th>1</th>
                                    <th>2</th>
                                    <th>3</th>

```

```

<th>4</th>
<th>5</th>
</tr>";
while($row = mysqli_fetch_assoc($result)) {
    $test_data[]=$row;
    $json['responses']=$test_data;
    $radioname = $row['id'];
    echo "<tr>";
    echo "<td id='radiobutton'>" . $row['id'] .
"</td>";
    echo "<td>" . $row['question'] . "</td>";
    echo "<td>" . $row['category'] . "</td>";
    for($i=1;$i<=5;$i++){
        echo "<td
id='radiobuttons'><input type='radio' name='$radioname' value='$i'></td>";
    }

    echo "</tr>";
}
echo "</table>";
}else {
    echo "<p id='complete'>No Questions in
the database!</p>";
    echo json_encode($json);
}
if(isset($_POST["submitbtn"])){
    $sql = "SELECT id, question FROM
forensicquestions";
    $result = mysqli_query($conn,$sql);
    while($row =
mysqli_fetch_assoc($result)) {
        $radio = $row['id'];
        @$_user_id = $_SESSION['user'];
        @$_forensicscore =
$_POST[$radio];
        if(@$_POST['submitbtn']){
            $sql="insert into
forensicassessments(userid,questionid,forensicscore)
values('$user_id','$radio','$forensicscore)";
            mysqli_query($conn,$sql);
            header("Location:
index.php");
        }
    }
}
?>
END... <input class="btn btn-default" type="submit"
name="submitbtn" value="Submit Results"

```

```

        onclick="return confirm('Are you sure you want to Submit?'); "
style="float:right;background:#132347;color:white;">
        </form>        </br></br></br>
    </div>
</div>
<?php include 'footer.php';?>

<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
<script src="assets/js/bootstrap.min.js"></script>

</body>
</html>

```

Evaluation

```

<?php
    ob_start();
    session_start();
    require_once 'dbconnect.php';
    if (!isset($_SESSION['user'])) {
        header("Location: login.php");
        exit;
    }
    $res = $conn->query("SELECT * FROM users WHERE id=" . $_SESSION['user']);
    $userRow = mysqli_fetch_array($res, MYSQLI_ASSOC);
    include('tcpdf/tcpdf.php');

    function fetch_data()
    {
        $user_id = $_SESSION['user'];
        $output = "";
        $conn = mysqli_connect("localhost", "root", "", "joycedb");
        //include_once 'dbconnect.php';
        $sql = "SELECT SUBSTRING_INDEX( c.username , ' ', 1 ) AS
user_name,a.assessmentdate,ROUND(((0.528+SUM(a.forensicscore *
b.categoryweight)+0.369)/(0.528+SUM(5 * b.categoryweight)+0.369)*100),0) as
effectiveness FROM forensicassessments a
                INNER JOIN forensicquestions b ON a.questionid=b.id
INNER JOIN users c ON a.userid=c.id group by c.id;";
        $result = mysqli_query($conn,$sql);
        while($row = mysqli_fetch_array($result))
        {
            set_time_limit(1800);
            $output .= '<tr>
<td>'.$row["user_name"].'</td>
                <td>'.$row["assessmentdate"].'</td>
                <td>'.$row["effectiveness"].'</td>

</tr>';
        }
        return $output;
    }

```

```

    }
    if(isset($_POST["create_pdf"]))
    {
        ini_set('max_execution_time', 180);
        ini_set('pcre.backtrack_limit', 1000000);
        require_once('tcpdf/tcpdf.php');
        $obj_pdf = new TCPDF('P', PDF_UNIT, PDF_PAGE_FORMAT, true,
'UTF-8', false);
        $obj_pdf->SetCreator(PDF_CREATOR);
        $obj_pdf->SetTitle("Forensic Adoptability PDF");
        $obj_pdf->SetHeaderData("", "", PDF_HEADER_TITLE,
PDF_HEADER_STRING);
        $obj_pdf->setHeaderFont(Array(PDF_FONT_NAME_MAIN, "",
PDF_FONT_SIZE_MAIN));
        $obj_pdf->setFooterFont(Array(PDF_FONT_NAME_DATA, "",
PDF_FONT_SIZE_DATA));
        $obj_pdf->SetDefaultMonospacedFont('helvetica');
        $obj_pdf->SetFooterMargin(PDF_MARGIN_FOOTER);
        $obj_pdf->SetMargins(PDF_MARGIN_LEFT, '5',
PDF_MARGIN_RIGHT);
        $obj_pdf->setPrintHeader(false);
        $obj_pdf->setPrintFooter(false);
        $obj_pdf->SetAutoPageBreak(TRUE, 10);
        $obj_pdf->SetFont('helvetica', "", 8);
        $obj_pdf->AddPage();
        $content = "";
        $content .= '
<h3 align="center">Forensic Adoptability PDF</h3><br /><br />
<table border="1" cellspacing="0" cellpadding="5">
    <tr>
        <th width="30%">Name of Assessee</th>
        <th width="30%">Date of Assessment</th>
        <th width="40%">Adoptability of Forensic
Tools(%)</th>
    </tr>
';
        $content .= fetch_data();
        $content .= '</table>';
        $obj_pdf->writeHTML($content);
        $obj_pdf->Output('Forensic Adoptability.pdf', 'I');
        // echo fetch_data();
    }
?>

```

APPENDIX IV: Permission to carry out Academic Research

NATIONAL POLICE SERVICE

Telegrams: "CRIMINAL" Nairobi
Email : pcorift@gmail.com
Tel : 2216773
Fax : 2217020



DCI REGIONAL COORDINATOR
RIFT VALLEY REGION
P.O. Box 2681
NAKURU

DIRECTORATE OF CRIMINAL INVESTIGATIONS

RCIO/SEC/1/2/1/11/VOL.I/57

30th January 2018

MS JOYCE C. CHEPKEMOI-GMIA/NE/0856/05/16
P.O BOX 1910
NAKURU

RE: PERMISSION TO CARRY OUT ACADEMIC RESEARCH

We are in receipt of your letter dated 28th January 2018 concerning your research project "Adoptability model for digital forensic evidence; a case study of Kenya Police Service" at Kabarak University in partial fulfillment of your M.Sc. in Information Technology Security and Audit degree. We appreciate your interest in our organization.

The National Police Service welcomes academic work in the appreciation that such work ultimately leads to better service to the Public. We notice that your research topics suggest it will be restricted to the Kenya Police Service.

In this regard, we suggest that you expand title to be the wider National Police Service, which comprises of: -

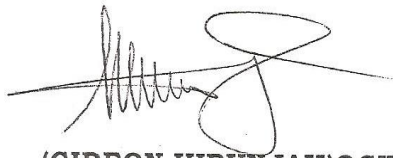
1. The Kenya Police Service
2. The Administration Police Service, and, most importantly,
3. The Directorate of Criminal Investigation (Most of the Forensic Science Specialized Sections are in the Directorate).

We will therefore accord you every support in your research project, subject to the work being used purely for academic purposes and the final product being shared with the Service.

You will therefore be expected to liaise with the Regional Coordinator DCI for details of the nature of your requirements from our personnel.

We have noted that you do appreciate that police matters are strictly of a confidential nature. Police officers are not authorized to disclose operational information and/or specific investigation details to third parties. You will therefore restrict your inquiries to general rather than specific areas.

You will therefore be expected to maintain strict confidentiality throughout your interactions with our staff. Should you require further clarification on this condition, or any other aspect of our support, kindly refer to the undersigned.

A handwritten signature in black ink, appearing to read 'Gideon Kibunjah', with a large, stylized flourish at the end.

(GIDEON KIBUNJAH)OGW
DCI REGIONAL COORDINATOR
RIFT VALLEY REGION

APPENDIX V: Research Authorization (NACOSTI)



NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone: +254-20-2213471,
2241349, 3310571, 2219420
Fax: +254-20-318245, 318249
Email: dg@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

NACOSTI, Upper Kabete
Off Waiyaki Way
P.O. Box 30623-00100
NAIROBI-KENYA

Ref. No. **NACOSTI/P/18/62258/21921**

Date: **26th March, 2018.**

Joyce Chepkemoi Chepkwony
Kabarak University
Private Bag - 20157
KABARAK.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on *“Adoptability model for digital forensic evidence in Kenya,”* I am pleased to inform you that you have been authorized to undertake research in **Nakuru County** for the period ending **23rd March, 2019.**

You are advised to report to **the County Commissioner and the County Director of Education, Nakuru County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit a **copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.


DR. M.K. RUGUTT, PhD, OGW
DIRECTOR GENERAL

Copy to:

The County Commissioner
Nakuru County.

The County Director of Education
Nakuru County.

APPENDIX VI: Research Permit (NACOSTI)

**THIS IS TO CERTIFY THAT:
MS. JOYCE CHEPKEMOI CHEPKWONY
of KABARAK UNIVERSITY, 0-20100
NAKURU, has been permitted to conduct
research in Nakuru County**

**on the topic: ADOPTABILITY MODEL
FOR DIGITAL FORENSIC EVIDENCE IN
KENYA**

**for the period ending:
23rd March, 2019**

.....
**Applicant's
Signature**

**Permit No : NACOSTI/P/18/62258/21921
Date Of Issue : 26th March, 2018
Fee Received :Ksh 1000**



.....
**Director General
National Commission for Science,
Technology & Innovation**

CONDITIONS

1. The License is valid for the proposed research, research site specified period.
2. Both the Licence and any rights thereunder are non-transferable.
3. Upon request of the Commission, the Licensee shall submit a progress report.
4. The Licensee shall report to the County Director of Education and County Governor in the area of research before commencement of the research.
5. Excavation, filming and collection of specimens are subject to further permissions from relevant Government agencies.
6. This Licence does not give authority to transfer research materials.
7. The Licensee shall submit two (2) hard copies and upload a soft copy of their final report.
8. The Commission reserves the right to modify the conditions of this Licence including its cancellation without prior notice.



REPUBLIC OF KENYA



**National Commission for Science,
Technology and Innovation**

**RESEARCH CLEARANCE
PERMIT**

Serial No.A 18065

CONDITIONS: see back page

APPENDIX VII: Research Authorization (County Commissioner)



THE PRESIDENCY
MINISTRY OF INTERIOR AND
CO-ORDINATION OF NATIONAL GOVERNMENT

Telegrams: "DISTRICTER", Nakuru
Telephone: Nakuru 051-2212515
When replying please quote

COUNTY COMMISSIONER
NAKURU COUNTY
P.O. BOX 81
NAKURU

Ref. No. **CC.SR.EDU 12/1/2 VOL.III/109)**

27th March, 2018

TO WHOM IT MAY CONCERN

**RE: RESEARCH AUTHORIZATION – JOYCE CHEPKEMOI
CHEPKWONY**

The above named student has been given permission to carry out research on ***"Adoptability model for digital forensic evidence in Kenya,"*** in Nakuru County for the period ending **23rd March, 2019.**

Please accord her all the necessary support to facilitate the success of her research.

**PATRICK OMUSE
FOR: COUNTY COMMISSIONER
NAKURU COUNTY**

APPENDIX VIII: Research Authorization (County Director of Education)

**MINISTRY OF EDUCATION
STATE DEPARTMENT OF EARLY LEARNING OF
BASIC EDUCATION**

Telegrams: "EDUCATION",
Telephone: 051-2216917
When replying please quote



COUNTY DIRECTOR OF EDUCATION
NAKURU COUNTY
P. O. BOX 259,
NAKURU.

Ref.CDE/NKU/GEN/4/21/VOL.VII/60

29TH March, 2018

TO WHOM IT MAY CONCERN

**RE: RESEARCH AUTHORIZATION -JOYCE CHEPKEMOI CHEPKWONY
PERMIT NO. NACOSTI/P/18/62258/21921**

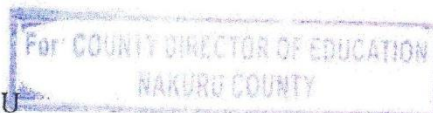
Reference is made to letter NACOSTI/P/18/62258/21921

Dated 26TH March, 2018.

Authority is hereby granted to the above named to carry out research on
*"Adoptability model for digital forensic evidence in Kenya in Nakuru
County,"* for a period ending
23rd March, 2019.

Kindly accord her the necessary assistance.

RUTH KAMAU
FOR: COUNTY DIRECTOR OF EDUCATION
NAKURU



Copy to:
Kabarak University
Private bag - 20157
KABARAK

APPENDIX IX: Introduction Letter (Kabarak University)



INSTITUTE OF POST GRADUATE STUDIES

Private Bag - 20157
KABARAK, KENYA
E-mail: directorpostgraduate@kabarak.ac.ke

Tel: 0773265999
Fax: 254-51-343012
www.kabarak.ac.ke

14th February 2018

Ministry of Higher Education Science and Technology,
National Council for Science, Technology & Innovation,
P.O. Box 30623 – 00100,

Dear Sir/Madam,

**RE: RESEARCH BY CHEPWONY JOYCE CHEPKEMOI-
GMIA/NE/0856/05/16**

The above named is a student at Kabarak University taking Master Degree in Information Technology Security and Audit. She is carrying out research entitled. “Adaptability model for Digital Forensic Evidence in Kenya.”

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide the necessary assistance.

Thank you.

Yours faithfully


Dr. Esther J. Kibor
AG DIRECTOR - (POST-GRADUATE STUDIES)

Kabarak University Moral Code

As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)



Kabarak University is ISO 9001:2015 Certified