ENHANCING CYBERCRIME INVESTIGATION EFFECTIVENESS: A MULTIFACETED ANALYSIS OF INFORMATION TECHNOLOGY TOOLS, DIGITAL EVIDENCE QUALITY, AND LAW ENFORCER SECURITY MEASURES

BY

BRIAN O. WASWA

MASTER OF SCIENCE IN INFORMATION SYSTEMS MANAGEMENT

KCA UNIVERSITY

2023

ENHANCING CYBERCRIME INVESTIGATION EFFECTIVENESS: A MULTIFACETED ANALYSIS OF INFORMATION TECHNOLOGY TOOLS, DIGITAL EVIDENCE QUALITY, AND LAW ENFORCER SECURITY MEASURES

BY

BRIAN O. WASWA

A DISSERTATION SUBMITTED IN PARTIAL FULLFILMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN INFORMATION SYSTEMS MANAGEMENT IN THE SCHOOL OF TECHNOLOGY AT KCA UNIVERSITY

OCTOBER 2023

DECLARATION

I declare that this dissertation is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this contains no material written or published by other people except where due reference is made and author duly acknowledged.

Student Name: Brian Waswa Reg No: 12/06955

Signature:  Date: 21st October 2023

I do hereby confirm that I have examined the master's dissertation of

Brian Waswa

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

X

Dr. Lucy Waruguru
mburul@kcau.ac.ke

Date: 22/10/2023

Dr. Lucy Waruguru Mburu

ACKNOWLEDGEMENT

I would like to extend my heartfelt acknowledgment to Dr. Lucy Mburu, whose guidance, expertise, and constructive feedback have shaped my research and academic growth. Your mentorship has been invaluable in helping me navigate through the challenges of this dissertation.

I am also grateful to my friends and colleagues, who have been a source of inspiration and motivation. Their solidarity and encouragement have lightened the burden and made this academic pursuit an enriching experience. Furthermore, I extend my acknowledgment to the law enforcement officers and participants who took part in the data collection process. Their willingness to share their insights and experiences has contributed significantly to the findings of this study.

DEDICATION

This dissertation is dedicated to my wife and kids for their unwavering support and unending love when I was weary and my spirit down.

I also wish to dedicate this work to my parents, whose constant encouragement and belief in my abilities have been a driving force throughout this academic journey. Their unwavering support and sacrifices have made this achievement possible.

Lastly, I dedicate this dissertation to all individuals affected by cybercrimes. It is my hope that this research contributes to the body of knowledge aimed at combating cyber threats and improving cybercrime investigation practices to protect individuals and organizations from the devastating effects of cybercrimes.

ENHANCING CYBERCRIME INVESTIGATION EFFECTIVENESS: A MULTIFACETED ANALYSIS OF INFORMATION TECHNOLOGY TOOLS, DIGITAL EVIDENCE QUALITY, AND LAW ENFORCER SECURITY MEASURES

ABSTRACT

In Kenya and in today's world, cybercrimes present a greater challenge in terms of detection and investigation compared to traditional crimes. As cybercrimes continue to evolve and become more complex, law enforcement agencies must continuously adapt their Information Technology tools to effectively combat this menace. These crimes have significant adverse effects on individuals' reputations, investors' finances, and data security. To prevent such damages, this study aimed to assess the application of Information Technology (IT) and propose a model applicable for investigating cybercrimes within the Directorate of Criminal Investigation (DCI) in Kenya. A case study approach was employed to explore the extent of Information Technology application in crime investigation, with a particular focus on using a regression model. Primary data was collected through the random distribution of questionnaires to 361 police officers from different units within the DCI department. The study developed a regression model that incorporated key variables, namely Information Technology tools, quality and quantity of evidence, and security of law enforcers The Pearson product-moment correlation was utilized to examine the associations among the study variables, while the regression model aimed to illustrate whether alterations observed in the dependent variable are linked to variations in the explanatory variables. The findings revealed that Information Technology Tools, Quantity and Quality of Evidence, and Security of Law Enforcers exhibited a positive and significant relationship with cybercrime investigation. Based on these results, it can be concluded that the utilization of Information and Communication Technology (ICT) tools has a positive and significant impact on the effectiveness of cybercrime investigation within the Department of Criminal Investigations (DCI) in Nairobi. The study recommended that the DCI conducts regular training sessions and workshops to keep investigators up to date with the latest technologies and their applications in cybercrime investigation. Additionally, future research should consider controlling for potential confounding variables that might influence the relationship between ICT tools usage and the effectiveness of cybercrime investigation.

TABLE OF CONTENTS

DECLARATION ..... **iv**

ACKNOWLEDGEMENT ..... **v**

DEDICATION ..... **vi**

ABSTRACT ..... **vii**

TABLE OF CONTENTS ..... **viii**

LIST OF FIGURES ..... **xi**

LIST OF TABLES ..... **xii**

ACRONYMS AND ABBREVIATIONS ..... **xiii**

THE OPERATIONAL DEFINITIONS OF KEY TERMS ..... **xiv**

CHAPTER ONE: INTRODUCTION **1**

1.1 Background of the Study 1

1.2 Cybercrime Models 5

1.3 Statement of problem 6

1.4 Objectives 7

1.4.1 General Objective 7

1.4.2 Specific Objectives 7

1.5 Research Questions 8

1.6 Significance of study 8

1.7 Scope and limitations of the study 10

CHAPTER TWO: LITERATURE REVIEW **11**

2.1 Introduction 11

2.2 Computer Forensics and The Development of Cybercrime 12

2.3 Cybercrime investigation 14

2.4 Cybercrime investigation in Kenya 18

2.4.1 Typical Cyber Intrusions 21

2.4.2 Serious Crimes 24

2.4.3 Cybersecurity Cycle Framework 26
2.5 Empirical literature review 27
2.5.1 Cybercrime investigation 27
2.5.2 ICT application on DCI 29
2.6 Theories of the study 31
2.6.1 Information Theory 31
2.6.2 Social Structure Social Learning Theory (SSSLT) 33
2.6.3 Routine Activity Theory 35
2.7 Variables influencing the application of IT tools 37
2.8 Conceptual Framework 39
2.9 Chapter summary 41
CHAPTER THREE: METHODOLOGY 42
3.1 Introduction 42
3.2 Research design 43
3.3 Study Area 43
3.4 Study Population 43
3.5 Sample of the study 45
3.6 Sampling design 46
3.7 Data collection 47
3.7.1: Validity of the Instrument 47
3.7.2: Reliability of the Instrument 47
3.8 Data Analysis 48
3.8.1 Analytical model 49
3.8.2 Diagnostic Tests 50
3.9 Ethical Considerations 52
CHAPTER FOUR: DATA ANALYSIS, FINDINGS, AND DISCUSSION 53
4.1 Validity and Reliability of Instrument 53
4.2 Questionnaire Response Rate 55
4.3 Demographics 55
4.3.1 Gender Distribution 55
4.3.2 Age Distribution 56

4.3.3 Respondents per Department 56
4.3.4 Respondents Years of Experience 57
4.3.5 Officers' Rank 58
4.3.6 Education Level 58
4.5 Descriptive Statistics 59
4.5.1 Impact of Information Technology Tool 59
4.5.2 Impact of Quality and Quantity of Evidence 60
4.5.3 Extent of Security of Law Enforcers 62
4.5.4 Effectiveness of cybercrime investigation 63
4.6 Inferential Statistics 64
4.6.1 Correlation Analysis 64
4.6.2 Multiple Regression Analysis 66
4.7 Diagnostic Tests 69
4.7.1 Autocorrelation Testing 69
4.7.2 Normality Testing 69
4.7.3 Multicollinearity Testing 71
4.7.4 Homoscedasticity Testing 72
4.7.5 Linearity Testing 73
CHAPTER FIVE: DISCUSSION, CONCLUSION AND RECOMMENDATIONS 75
5.1 Findings Summary 75
5.1.1 Information Technology Tools and cybercrime investigation 77
5.1.2 Quality and Quantity of Evidence and cybercrime investigation 77
5.1.3 Security of Law enforcers and cybercrime investigation 78
5.2 Conclusions of study 79
5.3 Implications for DCI and policy makers 80
5.4 Recommendations for Further Studies 82
REFERENCES 84
APPENDICES 93

LIST OF FIGURES

Figure 2. 1: Cyber threats detected in first quarter 2021 25

Figure 2. 2: Cyber threats detected in second quarter 2021 26

Figure 2. 3: Conceptual Framework 39

Figure 3. 1: Target Population in DCI 44

Figure 4. 1: ITT Normality Test 70

Figure 4. 2: QQE Normality Test 71

Figure 4. 3: SLE Normality Test 71

Figure 4. 4: ECI Normality Test 71

Figure 4. 5: Homoscedasticity Test 73

LIST OF TABLES

Table 2. 1: Operationalization of variables 40

Table 4. 1: Correlations 54

Table 4. 2: Reliability Statistics 54

Table 4. 3: Response Rate 55

Table 4. 4: Gender Distribution 56

Table 4. 5: Age Distribution 56

Table 4. 6: DCI Departments 57

Table 4. 7: Years of Experience 58

Table 4. 8: Rank 58

Table 4. 9: Education Level 59

Table 4. 10: Information Technology Tools 60

Table 4. 11: Quality and Quantity of Evidence 61

Table 4. 12: Security of Law Enforcers Descriptive Statistics 62

Table 4. 13: Effective cybercrime investigation Descriptive Statistics 63

Table 4. 14:Correlations 64

Table 4. 15:Model Summary 66

Table 4. 16: ANOVA[a] 66

Table 4. 17: Coefficients[a] 67

Table 4. 18: Autocorrelation Model Summary[b] 69

Table 4. 19: VIF Coefficients[a] 72

Table 4. 20: Linearity Test ANOVA Table 74

ACRONYMS AND ABBREVIATIONS

%	Percentage
AI	Artificial Intelligence
ANOVA	Analysis of Variance
APS	Administration Police Service
BWT	Broken Windows Theory
DBMS	Database Management System
DCI	Directorate of Criminal Investigation
DNA	Deoxyribonucleic Acid
HTML	Hypertext Markup Language
ICT	Information Communication Technology
IT	Information Technology
KCSR	Kenya Cyber Security Report
KPF	Kenya Police Force
KPS	Kenya Police Service
NPS	National Police Service
OSINT	Open-source intelligence
PHP	Hypertext Preprocessor
RAT	Routine Activity Theory
SLT	Social Learning Theory
SSSLT	Social Structure Social Learning Theory

THE OPERATIONAL DEFINITIONS OF KEY TERMS

IT TOOLS: A wide range of software, hardware, and equipment designed to assist individuals and organizations in various aspects of information technology. These tools are used to manage, create, store, manipulate, and communicate digital information and data (Researcher).

USAGE: The usage of IT (Information Technology) tools encompasses a wide range of applications and purposes across various industries and for personal use. IT tools are designed to perform specific tasks, enhance productivity, improve efficiency, and support various functions within the realm of information technology**.**

REGRESSION MODEL: A regression model is a statistical analysis tool used to examine the relationship between one or more independent variables (predictors) and a dependent variable (the outcome or response). The primary purpose of a regression model is to predict or explain the variation in the dependent variable based on the values of the independent variables.

CHAPTER ONE

INTRODUCTION

The chapter introduces background information on how the incorporation of IT (Information Technology) can increase effectiveness of cybercrime investigation in Kenya coupled with statement of problem and the study's general and specific objectives. Additionally, this chapter illustrates the research questions, outlines the study scope and significance of the research.

1.1 Background of the Study

1.1.1 Cybercrime Investigation in Kenya

In the 21st century, there have been innumerable challenges experienced by society due to the emergence of various forms of crime for instance; cyber-crimes have become very common unlike in the past (Khan et al., 2022). Paat (2020) in his study outlined that with the digital era on the rise, several risks including cyber-bullying, cyber-dating, human trafficking, internet fraud and bank fraud amongst others have emerged due to technological changes in the ecosystem. The mutation of these crimes brings in several challenges hence the need to adopt technology to enhance law enforcement practices. According to Asor (2020), factors like urbanization, migration to cities, and industrialization in the Philippines are the main attributes to high crime rates causing hindrance to economic development. When inequalities arise due to limited resources crimes tend to increase with the perpetrators engaging in technologically sophisticated crimes.

Subair et al. (2022) argued that due to contemporary concerns and alteration of crimes, the police must also invest on modern technologies to enable them tackle these crimes. Access to technological tools will enable the police to effectively execute their mandate. There are several

new developments with information technologies on investigation of crime such as video surveillance systems, Internet of Things (IoT), robots, DNA testing and other new technologies playing a vital role in crime investigation (Khan et al., 2022). While the application of technology is vital in crime investigation, examining the products involved in crime investigation is also very important. The application of modern technology in crime control is thus paramount and should be embraced.

The new global forms of crime such as cyberterrorism have generated new problems that the police officers must be prepared to effectively manage. According to Mwakio et al. (2020), Cyber-crime is a white-collar crime and involves an individual committing an illegal activity on the internet. Cybercrime is a common phenomenon around the world and it's due to the fast-ever-growing technological development, ability to commit and hide the traces of crimes remotely. The social interactions and businesses happening online offer it a platform for it to thrive.

As digital developments continue to rise, data attacks continue rising intensifying the effects of cyberterrorism therefore calling for strong frameworks to be put in place to counter-effect (Walumoli, 2021). According to Serianu (2020) Kenya Cyber Security Report (KCSR), cyber threats have increased from 2018 with malware, web application attacks taking the lead. These attacks lead to huge losses in terms of investments and savings on the victims. Farrow (2017) notes that local police officers are insufficiently able to deal with scam cases due to lack of resources to investigate internet fraud and other related crimes since they focus on crucial policing urgencies such as robbery, violent crimes, drug trafficking and burglary.

The Kenya policing system was inherited from British colonial rule with the National Police Service (NPS) succeeding the Kenya Police Force (KPF). NPS was introduced in the Constitution of Republic of Kenya in 2010 created to provide service to the public unlike KPF that

eroded public trust due to frequent use of unnecessary force and exhibiting unprofessionalism (Mbuba, 2021). The power to investigate crime in Kenya is vested in the Directorate of Criminal Investigations (DCI) that heads the Kenya Police Service (KPS) and Administration Police Service (APS). In Kenya, crime rates have continued to be rampant due to lack of ineffective tools of detection. The traditional approach to crime investigation was majorly via evidence from Deoxyribonucleic Acid (DNA), accounts of witnesses, and evidence from forensics. Additionally, complaints have been made against the Kenya police in relation to being undemocratic and lack of accountability.

Likewise, the Kenya police have low morale leading to increase in corruption through use of discretion to violate citizen's privacy and get away with it, detention of whoever they suspect to have violated law without reasonable cause, taking bribes and building cases against innocent people (Opalo, 2018). Such violations and corruption cases have contributed to lose of trust from citizens to the police. Investigation precedes arrest in a white-collar crime since law enforcers have to get a hint if there's something happening in a certain firm or on individual groups (Mwakio et al., 2020). Therefore, this implies that the law enforcement officers who manage crimes are required to be equipped with resources and trained to effectively manage these vices. The effects that cybercrimes place on an organization or individual are immense and can lead to people losing their bank savings, investors losing huge amounts of money to counter it amongst others. In Kenya, many cases of cyber-crime go unresolved due to few modern investigation equipment and unavailability of forensic laboratory (Mbaya, 2016). Worth noting is inadequate use of ICT in criminal investigation process in Kenya since the DCI have not fully utilized IT in their investigative operations to apprehend offenders (Mwakio et al., 2020). According to Tanui and

Barmao (2016), DCI, Kenya has not fully established and utilized tools for crime detection and prevention due to maintenance difficulties by the police.

The Cybercrime Act plays a pivotal role in shaping the landscape of cybercrime investigation research in Kenya. The Cybercrime Bill originated from the Office of the Director of Public Prosecutions (ODPP). Its primary aim was to provide law enforcement agencies with essential legal and forensic resources for addressing cybercrime, an issue estimated to have inflicted an economic toll of approximately KES 2 billion (USD 23 million) on the Kenyan economy in the year 2013. Enacted in 2018, the Act encompasses legal provisions that are crucial to understanding and addressing cybercrimes within the country's jurisdiction. One of the key aspects that highlight its relevance is its definition of various cyber offenses, which provides a clear framework for categorizing and prosecuting different types of cybercrimes. This definition not only guides law enforcement agencies but also forms the foundation for research efforts aimed at studying the prevalence, nature, and impact of cybercrimes in Kenya.

Moreover, the Cybercrime Act outlines procedures for the collection, preservation, and presentation of electronic evidence in court. This procedural guidance is essential for researchers engaged in cybercrime investigation research, as it informs them about the legal standards and requirements governing the admissibility of digital evidence. Understanding these protocols is paramount for researchers seeking to develop methodologies for effectively collecting and handling digital evidence in a manner that aligns with legal expectations.

Additionally, the Act underscores the importance of international cooperation in tackling cybercrimes, enabling researchers to explore the dynamics of cross-border cybercrime investigations and the challenges associated with them. Furthermore, the Act's provisions related to the protection of critical information infrastructure and the establishment of a National

Computer and Cybercrimes Coordination Committee demonstrate its relevance to research on strategies for safeguarding critical digital assets and coordinating efforts among various stakeholders in cybercrime investigation.

In essence, the Cybercrime Act significantly shapes the research landscape in Kenya by providing a legal framework that defines cyber offenses, outlines procedures for evidence handling, and establishes mechanisms for international collaboration. Researchers investigating cybercrime in Kenya benefit from this Act as it not only informs their studies but also encourages the development of effective strategies to combat cybercrimes while upholding legal standards (*The Computer Misuse and Cybercrimes Act – NC4, 2018*).

1.2 Cybercrime Models

Cybercrime model is an abstract framework of reference of any independent technology for supporting investigators work (Ciardhuáin, 2004). A model provides a common ground for discussion on expertise exchange and technology share to proactively identify opportunities for future deployment of technology in various firms (Adesina et al., 2022).

Lee et al. (2001) in San Diego developed an investigative model known as the scientific crime scene investigation. According to the model, scientific cyber scene investigation is a process that has 4 steps; recognition, identification, individualization, and reconstruction. This model emphasized a methodological and systematic investigation process using physical evidence. However, this model has suffered limitations since it only refers to the forensic part of investigation while neglecting the aspect of exchanging information with other investigators (Wekundah, 2015). Similarly, Reith et al. (2002) introduced a model that was consequential of Digital Forensic Research Workshop model.

The key activities in the model are; identification, preparation, approach strategy, preparation, collection, examination, analysis, presentation and return of evidence. This model can be a reference point in development of techniques to be used in investigation. Its major drawback is that it emphasizes on the investigation process after a cybercrime has occurred (Ciardhuáin, 2004). Valjarevic and Venter (2012) in South Africa developed a harmonized digital forensic investigation process model aimed at complementing existing models. The model inherited most of the phases by prior authors making it comprehensive and adopts a novel approach to implement some digital forensic principles. It comprises 12 phases; incident detection, first response, planning, preparation, incident scene documentation, potential evidence identification, potential evidence collection, potential evidence transportation, potential evidence storage, potential evidence analysis, and presentation. This model is substantially generic to be used in different digital forensic investigations with various types of digital evidence. Wekundah (2015) developed a model that sought to improve on existing models, report and reference cybercrime strategies towards SMEs in Kenya. The model had key steps; prevention and early warning, detection, reaction, and crisis management. This model exists to assist prior to a cybercrime investigation.

From the above prior existing models proposed by various authors related to cybercrime investigation, most models have laid focus on collection and preservation of digital evidence while some outline basic investigative processes of any crime. Therefore, this study seeks to develop a more proactive and comprehensive model to be adopted prior and during cybercrime investigation process.

1.3 Statement of problem

The pervasive adoption of digital technology has led to a surge in internet users in various domains, resulting in the emergence of cybercrime (Khweiled, 2021). Cybercrime has evolved

rapidly, notably during the global COVID-19 pandemic in the last quarter of 2019 when traditional crime rates decreased due to curfews, but cybercrimes escalated (Khweiled, 2021). Increased online activities, remote work, and e-commerce provided fertile ground for cybercriminals.

Despite this rise in cybercrimes, the police and investigators in Kenya have been slow to embrace modern technology for investigations, adhering to traditional methods, which are increasingly ineffective in the age of technology (Odoyo et al., 2020). This disconnect between the evolving nature of cybercrimes and the investigative techniques necessitates significant attention.

The gap in the literature becomes evident when examining the localized threat landscape and unique challenges faced by cybercrime investigators in Kenya. There's also a lack of regression models tailored to the field of cybercrime investigation, which is crucial for addressing the evolving nature of digital crimes (Kader and Minaar, 2015). This study aims to fill these knowledge gaps by creating a regression model that enhances our understanding of the investigative process within the context of cybercrimes, addressing the need for hypothesis testing and in-depth exploration of core variables (Zhang and Lei, 2022; Rupa et al., 2020; Udanor et al., 2020).

1.4 Objectives

1.4.1 General Objective

To determine how Information Technology Tools, Quality & Quantity of Evidence, and the Security of Law Enforcers individually and collectively influence the effectiveness of cybercrime investigations.

1.4.2 Specific Objectives

The specific objectives guiding this study include:

i. To assess the impact of Information Technology Tools on the effectiveness of cybercrime

investigations.

ii. To evaluate the influence of Quality & Quantity of Evidence on the effectiveness of cybercrime investigations

iii. To investigate the relationship between the Security of Law Enforcers and the effectiveness of cybercrime investigations

1.5 Research Questions

The research questions guiding this study include:

i. How do Information Technology Tools affect the effectiveness of cybercrime investigations, and which critical factors within these tools contribute to improved outcomes?

ii. What is the relationship between the Quality & Quantity of Evidence and case resolution in cybercrime investigations, and which procedures lead to higher-quality digital evidence?

iii. To what extent does the Security of Law Enforcers influence the overall effectiveness of cybercrime investigations, and which security measures have the most significant impact on outcomes?

1.6 Significance of study

This research contributes enormously towards present information within the areas of information technology as well as use of regression model in cybercrime investigation. This research additionally contributes towards the inadequate number of empirical researches on quality and quantity of evidence, information technology, security of law enforcers' depending on the effectiveness of cybercrime investigation.

The research avails additional understanding on the dangers of cybercrime to Information System experts in so doing assisting in undertaking research, preparation, formulating, as well as enhancing computer-based mechanisms, software and associated to sustain information systems easier through confirming integrity and data security.

This study anticipated gauging the application of information technology in cyber-crime investigation in Kenya with the case study on DCI. This highlights the great benefits of information technology in investigations hence encouraging more investments for the benefit of the police officers. The study will also reveal problems that the DCI encounter while performing criminal investigation activities and outline how ICT helps.

The findings from this study is important in aiding the DCI and the NPS in evaluating the uptake of technology and identification of the various areas of weakness in technology implementation aimed at effective cybercrime investigation and justice. Additionally, this study developed a model of information system for criminal investigation to be used so as to improve the cyber-crime investigation process.

This study also serves as a guide to policy makers, the NPS and DCI to formulate strong policies and approaches that help in adoption of technology in cybercrime prevention. Similarly, the researcher provides more insight to the public on the damaging effects of cybercrime to the economy to help mitigate it. The information obtained is a great addition to the existing literature on the use of technology in crime investigation in the sub-Saharan side of Africa. The findings will be very critical to the future researchers who intend to study a similar topic as a literary work.

1.7 Scope and limitations of the study

The study was focused on the Directorate of Criminal Investigations, a department of the Kenya National Police Service. The study intended to explore how the DCI have incorporated various technology tools in the fight against cybercrime. The study also sought to determine the impact of information technology in preventing the rate at which cybercrimes are committed. Finally, it meant to assess the problems faced in application of ICT in investigation and the extent of information technology in DCI especially among the police officers in collecting evidence.

This study was however restricted to the NPS in Kenya especially on the department of DCI in Nairobi. The main aim for selecting DCI is due to the fact that it is the backbone of NPS and is also the department given the mandate to conduct criminal investigations. (Mbuba, 2021) DCI also heads the Kenya Police Service (KPS) and Administrative Police Service (APS). Similarly, selecting Nairobi is due to financial and time constraints from the researcher's side and also due to the fact that most crime rates are high in urban areas especially in cities (Ndikaru, 2021)

CHAPTER TWO

LITERATURE REVIEW

This study's chapter analyzes the literature associated with the study's theme. It additionally looks into the previous philosophers' thoughts on the subject. The empirical review is fixated on study determinants therefore through literature reviewing under the sub-themes enables synchronization with the objectives of research. Additionally, it depicts associations acknowledged by prior scholars. The chapter is organized in four main areas; introduction, empirical review, theoretical review, and the conceptual framework.

2.1 Introduction

Information Technology (IT) is a broad title that describes wide array of technologies used to store, retrieve, process, gather, analyze and transmit data or information. It generally encompasses the software, hardware and networks used in collecting, storing, processing and transmitting data. According to Okutan (2019), there are ever-rising technologies in the field of IT and its emergence has generated social, cultural and economic dynamics. ICT tools include fax, radio, computers, internet, internet cables, routers, switches, CCTV, and telephones among others (Bamanyisa, 2018).

Advanced technologies and IT are becoming powerful tools in measuring performance, solving problems, policing among other functions. These technologies bear the highest potential on control especially in developing countries like Kenya. Greater efficiency and accountability in achieving urban security is through introducing information technology-based actions (Samoei, 2018). Although with the continued rise of information technologies, a major challenge that is experienced is the willingness to adopt it for various functions. Good governance and efficiency

can be achieved in Kenya through embracing these technologies since every crime in our society has a technological aspect to it (Odoyo et al., 2020).

Cybercrimes encompass illicit activities perpetrated in the digital realm through the utilization of computer and network technology facilitated by Information and Communication infrastructures. Evident patterns have demonstrated that the capacity of law enforcement to expand their operations has been insufficient to adequately address the emerging complexities presented by Cybercrime, which endangers the welfare of diverse Internet user groups. The scope of Cybercrime has transcended geographical confines, and nations lacking comprehensive or absent legislation pertaining to cyber criminals are progressively becoming more susceptible to cyberattacks.

In Kenya, the NPS faces pressure from the media, public, investors and government on the unethical practices and corruption happening through cybercrime bringing down the country's development. The trends of cybercrimes have continued to heighten despite the legal powers bestowed on the DCI to conduct investigations (Mwakio et al., 2020). Therefore, Information Technology proves to be the solution of bringing efficiency and effectiveness in the investigation process.

2.2 Computer Forensics and The Development of Cybercrime

The introduction of computers in the mid-1940s marked a significant milestone. However, this rapid advancement was accompanied by a surge in various computer-related offenses. Despite numerous incidents, many offenses remained undisclosed, unprosecuted, or obscured from the general public (Khan et al., 2022). The 1970s and 1980s witnessed the proliferation of personal computers, as both individuals and businesses integrated them into their routines. This growing

reliance on computers led to the recognition of Cybercrime by law enforcement agencies in technologically advanced nations by the 1990s. Systems were instituted to facilitate investigation and prosecution, laying the foundation for Computer Forensics. As early as 1984, the FBI laboratory in the United States and other law enforcement bodies-initiated programs to aid in the examination of computer evidence. This response was primarily driven by the escalating demands of investigators and prosecutors. The objective was to methodically address these demands, culminating in the formation of the Computer Analysis Response Team, or CART (Horgan et al., 2021).

Over the past decades, Computer Forensics has evolved into a discipline that identifies, resolves, documents, and supports the prosecution of computer or cybercrimes. From the 1960s to the present day, Computer Forensics has transitioned from an era lacking proper structure, well-defined goals, sufficient tools, processes, and procedures to an era characterized by structured frameworks, accepted protocols, and specialized tools designed to facilitate the wide application of digital evidence within legal frameworks (Communications, 2021). Today, real-time digital evidence collection is feasible, accompanied by the development of field collection tools. Moreover, forensics has extended its reach to encompass the Legal, Military, Private Sector, and Academic domains. Despite these advancements, however, there are multiple factors that can impede a successful investigation and prosecution. According to Chang, Kuo, and Ramachandran (2016), the predominant factor is lack of preparation. Investigative organizations often lack the necessary tools and expertise to effectively gather evidence. In cases where individuals attempt investigations, they might lack the requisite resources or tools to conduct a thorough inquiry, ensuring the irrefutability of evidence in all scenarios (Garcia, 2018).

Furthermore, situations arise when organizations have adequately established the required tools, skills, and resources, but due to insufficient training and improper procedures, collected evidence becomes susceptible to dispute (Khan et al., 2022). The landscape of Cybercrime is also experiencing significant evolution, propelled by the online opportunities that contribute to its widespread growth and its consequential detrimental impacts. This evolution is linked to the increasing trend of criminal entities utilizing the internet to facilitate their activities, with a primary focus on rapidly maximizing profits.

2.3 Cybercrime investigation

According to Šarūna and Jevgenijus (2020), Cybercrime is a distinct crime whereby a criminal uses computer technology to access business secrets, personal information or use the Internet for malicious activities. The perpetrator uses the internet as an opportunity to commit illegal acts. Odoyo et al. (2020) in their study highlighted an investigative process as an activity involving collection of evidence, examining data, analyzing and reporting the incident. Additionally, Investigation of a crime scene is a process that the judicial detects and examines in accordance with the law to understand the circumstances surrounding the case and amass relevant evidence (Wu et al., 2019).

Cybercrime typically revolves around two primary categories of offenses. In one category, the offense targets a computer connected to a network, exemplified by attacks on network confidentiality, integrity, and/or availability (Magutu et al., 2011). The other category encompasses conventional crimes like theft, fraud, and forgery, which are committed using computers connected to networks, computer networks, and associated information and communications technology.

Cybercrime can be defined as any criminal activity that is facilitated or executed utilizing a computer, network, or hardware device. The computer or device can act as the perpetrator of the crime, assist in the commission of the crime, or be the target of the crime itself. This criminal activity can transpire solely within the digital realm or extend to physical locations beyond the virtual sphere.

Unauthorized access to hosts, commonly known as hacking, manifests in various forms, some of which may not always demand extensive technical expertise. This involves the utilization of computers or terminals to breach the security of certain computer systems. Cybercriminals employ methods such as snifting or password guessing to breach security, thereby significantly weakening the effectiveness of passwords when users do not exercise judicious selection.

Spamming entails inundating the internet with numerous copies of identical messages sent to multiple addresses. The spammer dispatches millions of emails with the expectation that a small percentage will reach recipients' inboxes and an even smaller fraction will elicit responses. These spam messages are invariably sent with falsified return address information, often referred to as junk mail.

Among the more prevalent forms of computer fraud is manipulation-based fraud, where intangible assets represented in data formats, such as monetary balances or work hours, constitute the prime targets. In the contemporary business landscape, monetary transactions are increasingly reliant on computer systems, offering substantial opportunities for computer-related fraud. Organized criminal entities have also homed in on credit card data, alongside personal and financial information, which they sell to counterfeiters of credit cards and travel documents, proving to be immensely profitable.

Viruses, Trojans, and Worms all fall within the same category as they are software entities designed to infect computers or implant themselves onto systems without user authorization. Their operational mechanisms, however, diverge significantly. A typical virus engages in two primary activities: firstly, it replicates itself into previously unaffected programs, and secondly, it executes additional instructions embedded by its creator. Some viruses may lack harmful instructions altogether, causing disruption solely by replicating and consuming disk space.

Another significant facet of cybercrime pertains to piracy, which involves the unlawful duplication of movies, games, software, music, and other digital media. Piracy is often straightforward, frequently necessitating nothing more than a CD-RW or DVD-R/RW drive to reproduce original CDs or DVDs that store applications. Alternatively, music, games, and applications can be readily copied onto the internet for downloading.

Furthermore, cyberstalking and cyber-harassment constitute persistent, targeted harassment through electronic communication channels such as email. Cyberstalking is defined as the recurrent use of the Internet, email, or associated digital electronic communication devices to distress, alarm, or threaten a specific individual.

Cybercrime investigation refers to the practice of screening, secret and on-site investigation, electronic evidence collection, evidence analysis and extraction of a cybercrime case by authorized criminal investigation and law enforcement bodies. These procedures are carried out to determine if a crime was committed, identify and arrest the criminal, and provide evidence to support court trial. Improving on investigative methods and techniques is a key to detecting cybercrimes since they are challenging to obtain evidence and apprehend the perpetrators (Wu et al., 2019). Besides assessing the crime scene, law enforcers examine artifacts from the crime scene to determine the person(s) of interest. Cybercriminals often leave fingerprints that can be traced to

internet cache, log files, signatures among others which help identify character patterns and traits on how the criminal carried out the crime (Garcia, 2018).

The significance of a robust cybercrime investigation model lies in its capacity to provide an abstract and universal reference framework, detached from specific technologies or organizational contexts. This framework serves as a foundation for deliberations concerning techniques and technologies that facilitate the endeavors of investigators. Notably, it establishes a shared vocabulary, fostering discourse and the exchange of expertise. The model's utility extends to guiding the creation and application of methodologies relevant to emerging technologies that come under investigative scrutiny.

Moreover, the model serves a proactive purpose by identifying prospects for the development and deployment of technology geared towards supporting investigative efforts. It furnishes a structured approach to capturing and scrutinizing requisites for investigative tools, especially those of an advanced automated analytical nature. Presently, a conspicuous absence of comprehensive models tailored explicitly for cybercrime investigations is evident. Although existing models target specific facets of the investigative process such as evidence collection, analysis, and presentation; a comprehensive model must encompass additional dimensions to offer a truly comprehensive perspective.

The creation of a robust cybercrime investigation model holds great importance as it provides an abstract and versatile framework for discussions, shared understanding, and the application of techniques pertinent to investigative work. By accommodating diverse technological landscapes, this model can effectively guide the implementation of methodologies and facilitate the development of supportive technologies. Furthermore, its application transcends the domain of law enforcement, extending its advantages to IT managers, security practitioners,

and auditors confronted with the escalating complexities of investigating various forms of misconduct.

A beneficial standpoint of cybercriminal investigation is provided by Broken Windows Theory (BWT) in scrutinizing the influence of information technology on crime investigation. According to Jiang et al. (2018) this theory was introduced by Wilson and Kellings in 1982 in a theory-based context that crime investigation is influenced by the social environment. BWT explores how environmental conditions can shape people's opinion and crime levels in an environment. The conditions in the environment have shown crime induction and leading average citizens to withdraw causing societal decay and quality of life to decline. This theory demonstrates that disorder influences people's perception in safety. BWT advocates that for this cycle to be broken, disorders in the environment need to be removed and order established to improve perceptions in the society. The core idea behind the broken windows theory is the crime prevention approach through intervening on causal factors that lead to crime incident. It puts emphasis on prevention of crime and its negative results which does not escape this study. This study seeks to assess the elimination of crime through adoption of IT.

2.4 Cybercrime investigation in Kenya

Over an extended duration, the evolution of digital forensics in Kenya has primarily revolved around tools generated by commercial developers to facilitate computer investigation procedures. The convergence of this approach, coupled with the absence of established standards guiding cybercrime investigators within this realm, has engendered concerns related to the dependability, verifiability, and consistency of digital evidence when presented in legal proceedings (Hewling, 2013). The absence of standardized protocols becomes particularly

conspicuous in instances where the anonymity inherent in online activities hampers the identification of cyber incident authors, due to the lack of universally recognized procedures. Despite the existence of multiple forensic models at present, the field has been further complicated, as the currently available procedures authored by different individuals exhibit significant disparities that impede the investigative process (Lalla et al., 2010). It is the dearth of standardized investigation procedures that frequently enables low-level offenders to operate without challenge. A report by police executive research forum (2014), indicated that this phenomenon arises as law enforcement agencies disproportionately allocate their limited resources toward major cases, consequently placing enforcement personnel in challenging situations when dealing with cybercrime investigations.

Consequently, there exists a pressing need for Kenya to establish legislation that furnishes a framework encompassing standards, principles of quality, and methodologies for the identification, preservation, retrieval, examination, and admissible use of digital evidence for forensic purposes. Simultaneously, regulations governing training and certification must be put in place to encourage uniform investigative methodologies, yielding more consistent outcomes. This initiative aims to firmly integrate computer forensics into the fabric of Kenyan evidentiary law. Furthermore, the police and other law enforcement entities will require these specialized techniques and protocols to proficiently conduct investigations, analyze information, and construct computer systems equipped to ascertain the timing, methods, and perpetrators of computer-related offenses (Wanderi, 2007).

Kenya National Police Service (NPS) is a body that draws its mandates from the National Police Service Act Section 11A of 2011. The NPS oversees law enforcement, prevention of crime, recruitment and deployment of police. Despite having a devolved government, the policing system

is not devolved and it's the Inspector General who issues all the command. NPS is comprised of three branches; the DCI, APS and KPS who have identical chain of command (Mbuba, 2021). The police are required to be; representative and accountable to the communities they serve, ethical and offer transparency in their activities and protect the rights and safety of individuals. The DCI is the department given the mandate to conduct criminal investigations and is headed by a Director who is appointed by the President. The DCI derives its mandate from Article 247of the constitution of Kenya in the National Police Act 2011, Part V, Section 28 and 35(National Police Service Act, 2011).

In Kenya, instances of cybercriminal attacks have been witnessed, with comparatively less attention directed towards business entities that fall victim. According to a Synovate report, the country has encountered significant attacks in recent years (Wekundah, 2015). Examples include the cyber assault on the Central Bank of Kenya in 2013, the breach of 5,000 Facebook Kenyan accounts orchestrated by cybercriminals, and the NIC bank incident involving the prosecution of an employee who misappropriated over 2.8 million Kenyan shillings. Notably, while some cases have gained public attention, such as the temporary hijacking of Hope FM radio station by cybercriminals in January 2015, many other occurrences remain undisclosed. The recent cyber incidents targeting Egerton University and the E-citizen website exemplify this trend. The underlying rationale for maintaining silence about these attacks primarily stems from the potential risk of eroding business credibility in the eyes of customers. In certain instances, businesses might not even be aware of the attacks unless the financial repercussions become palpable (Wekundah, 2015). Consequently, many businesses opt to manage cyberattacks discreetly and focus on recuperation to safeguard customer relationships.

The investigation process of cybercrimes encompasses the sequential stages of evidence gathering, data scrutiny, analysis, and eventual reporting in response to incidents (Mbuba, 2021). Kenya is currently undergoing a transitional phase in addressing cybercrime. However, akin to many other nations, local law enforcement agencies are encountering cultural challenges in their approach to cybercrime investigation, particularly in the shift from conventional investigative techniques to methods suited for handling cyber offenses. The integration of cybercrime investigation practices has encountered resistance, with a lingering inclination towards managing traditional forms of criminal activity.

Regrettably, cybercrime has evolved into an issue that demands thorough preparedness from officers or investigators entrusted with its resolution. To effectively combat cybercrimes, investigators must acknowledge that nearly every contemporary offense within our communities harbors a technological dimension. Consequently, it is imperative for police departments to embrace this evolving landscape and equip themselves to counteract cybercrime. According to a report by police executive research forum (2014), this entails comprehending the mechanisms of cybercrime commission and the necessary actions to undertake in the event of an incident. Notably, the dynamic evolution of cyber threats influences policing in three key dimensions: the workload imposed on law enforcement related to cybercrime, the quality of public service delivery, and the police administration's capacity to effectively execute its duties.

2.4.1 Typical Cyber Intrusions

A plethora of cyber intrusions exist, most of which stem from the internet's network connectivity. As highlighted by Akers et al. (2016), there exists a range of attack modalities that pose vulnerabilities to various organizations.

2.4.1.1 Disruption through Denial of Service

Denial of Service (DoS) attacks operate with the intention of preventing or diminishing the legitimate user's capacity to access a service or network resource. These attacks can even result in the impairment or shutdown of the server providing such services. DoS attacks can be categorized into two principal types: service incapacitation attacks and resource degradation. Various sources, including the annual UNESCAP report on computer crime and Adesina et al. (2022), indicate that Distributed Denial of Service (DDoS) attacks have imposed substantial financial burdens on companies in recent times. Furthermore, they adversely impact consumer trust in the e-commerce operations of affected organizations.

A range of DDoS attack variants exists. They all conform to a common structural pattern, illustrated in the diagram below. The assailant initiates a DDoS assault by initially compromising multiple master computers linked to wireless networks, often through hacking methods. These master computers then extend their control to additional computers, referred to as zombies, using diverse techniques. Subsequently, the attacker dispatches a directive to synchronize all zombies, compelling them to direct the targeted traffic towards the victim.

2.4.1.2 Incidents of Phishing

Criminal entities operating in the digital realm have been observed creating counterfeit websites resembling authentic ones, with the intention of extracting data from site users (Collier, 2020). The deception involved in phishing scams involves the fabrication of fraudulent web pages, emails, or text messages, strategically designed to entice unsuspecting users into divulging sensitive data like passwords, financial particulars, and other private information.

Historically, cyber criminals have successfully harvested personal data from online users by presenting them with imitation pages, strategically targeting online customers and siphoning their

personal data. This act, commonly known as phishing, involves the direct capture of details or the dispatch of emails to users, deceitfully notifying them of their credit card's impending expiration.

2.4.1.3 Malicious Software Incursions

Malicious software attacks, commonly known as malware attacks, refer to the deployment of harmful software or applications that disrupt the normal functioning of computers. According to references from Akers et al. (2016) and Adesina et al. (2022) along with Collier (2020), diverse types of malware attacks are prevalent, as outlined below:

1. Trojans: Trojans represent a category of malware that executes unauthorized and often malevolent actions. The key distinction between a Trojan and a virus lies in the Trojan's inability to self-replicate.
2. Viruses: Viruses constitute a code sequence that infiltrates and embeds itself within another executable code. Consequently, when the regular program is executed, the viral code also activates.
3. Worms: Worms are programs designed to autonomously create duplicates of themselves, typically through various methods such as email or other transmission mechanisms.

2.4.1.4 Man in the Middle Compromises

This form of attack endeavors to position the aggressor within a communication exchange, aiming to intercept a client's data, modify it, and subsequently either discard the data or transmit it to the authentic destination. As outlined by O'Hanley (2013), two primary variations of intermediary compromise tactics are identifiable:

- Manipulation maneuvers: This involves the capacity to manipulate and subsequently retransmit altered data. Furthermore, Spoofing Attacks, such as Mac address spoofing, IP spoofing, or frame spoofing, also fall within this category.

- Eavesdropping assaults: These entail the unauthorized acquisition of network information via wireless signals, commonly referred to as Sniffing Attacks.

2.4.2 Serious Crimes

In contemporary times, a significant majority, exceeding 60 percent, of commercial transactions are conducted via online platforms. This paradigm shift towards digital engagement necessitates a heightened emphasis on security measures. The domain of cybersecurity extends beyond safeguarding information solely within the IT industry, encompassing a wide spectrum of sectors including cyberspace. Even cutting-edge technologies such as mobile computing, cloud computing, online banking, and E-commerce are not exempt from the imperative of robust security, as they house critical information pertaining to individuals, for whom security has become an indispensable requirement.

The Internet has increasingly become a conduit for sophisticated criminal activities orchestrated by organized crime groups. This trend has seen a migration away from conventional criminal methodologies towards internet-based crime, which is gaining prominence. This is exemplified by the involvement of organized crime in white-collar criminal activities, a sphere previously distinct. Instances of internet-based stock fraud have reaped substantial illicit gains for criminals, resulting in financial losses for investors. Consequently, this realm has evolved into a highly profitable arena for such nefarious undertakings.

Enhancing cybersecurity measures and fortifying the protection of sensitive information assumes paramount importance for the safety and economic prosperity of every nation. The imperative of rendering the Internet a safer realm has become inextricably linked with the advancement of new services and the formulation of governmental policies. The battle against cybercrime necessitates a comprehensive and multifaceted approach. Acknowledging that

technological safeguards alone cannot entirely preclude criminal activities, it becomes imperative to empower law enforcement agencies to diligently investigate and prosecute cybercrime.

In the present landscape, numerous nations and governments have implemented stringent legislative frameworks to curb these losses. Beyond legislative measures, it is incumbent upon everyone to cultivate proficiency in cybersecurity. This imperative is underscored by a discernible surge in reported cybercrimes, a trend confirmed by police departments across various nations.

The DCI is a department under NPS that is concerned with investigation of crimes and takes instructions from the Inspector General of the Republic of Kenya. Worth noting is the major responsibility of the DCI to investigate serious crimes like cybercrime, piracy, terrorism among others. The DCI is thus a special organ that conducts investigations on serious crimes. For this cause, it should possess special investigative ICT tools to conduct efficient forensic analysis.

In a recent quarterly report by Communications Authority (CA) of Kenya shows an increase of cyber threats by a round off of 269% in July to September 2021(Communications Authority, 2021). This was attributed to adoption of more sophisticated tools by actors of cyber threat, increased activity by ransomware groups, increased attacks of IoT devices amongst others.

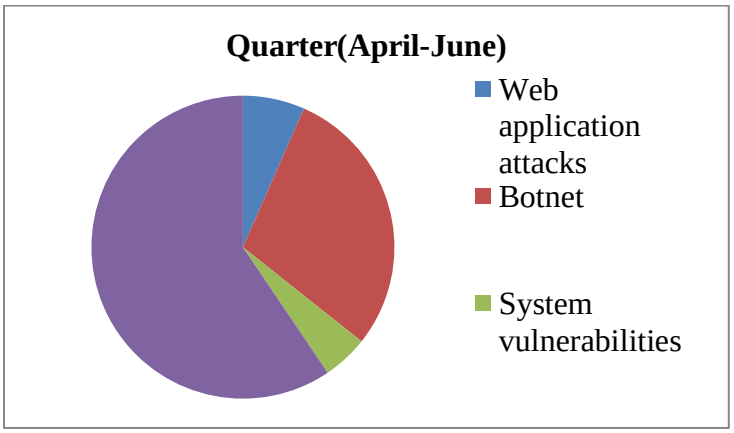

Figure 2. 1: Cyber threats detected in first quarter 2021

Source: CSSR Q1 (2021)

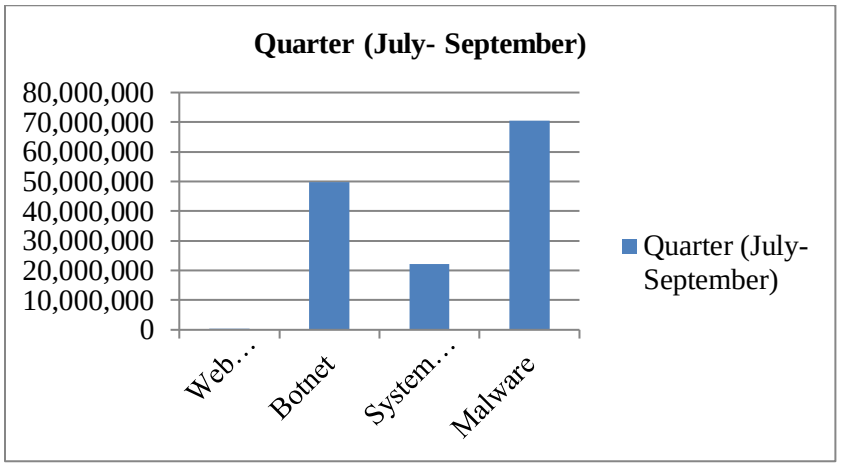

Figure 2. 2: Cyber threats detected in second quarter 2021

Source: CSSR Q1 (2021)

Statistically, the number of cyber threats reported is continuing to rise evident from the above diagrams. This predicts the magnitude of work the DCI have to put in to curb such events from arising in future. Cybercrimes are complex in nature leading to economic deterioration and rising fear of crime. From the above report, there appears a persistence need to acquire or upgrade existing IT tools to improve on the investigation process to ultimately achieve a secure cyberspace.

2.4.3 Cybersecurity Cycle Framework

Given the potential for prolonged harm over time, any comprehensive cybersecurity strategy must be firmly rooted in the framework of the cybersecurity cycle (Wekundah, 2015). This cycle encompasses the following three distinct phases as illustrated by Zaballos, and Herranz, (2013):

- Readiness and Prevention:

This initial phase revolves around equipping both human users and computing systems to shield themselves from various cyber threats. It concurrently emphasizes the enhancement of security measures and the avoidance of vulnerabilities inherent in specific technologies.

- Identification:

The subsequent stage entails the swift identification of potential threats, aiming to minimize the time gap between the emergence of a threat and its detection.

- Response:

This final phase pertains to the prompt recognition and rectification of the root causes underlying a disruption.

By embracing this comprehensive approach, a holistic perspective on Cybercrime can be achieved. All relevant facts are brought under scrutiny to effectively address the complexities associated with cyber threats (Wekundah, 2015).

2.5 Empirical literature review

2.5.1 Cybercrime investigation

Cybercrime investigation involves the process of screening the site of criminal activity, collecting evidence, analyzing and reporting the evidence materials (Wu et al., 2019). Cybercrime investigation process raises the need to improve on the intelligent technologies to keep pace with the developments in the environment. Cybercrime has posed sophisticated challenges since the crimes are difficult to trace back to the perpetrators while some erasing their digital footprints (Mmabatho & Mofokeng, 2021)

Horan and Saiedian (2021) in their research notes digital forensics and online investigations as major technologies and methods used to gather data in cyber investigations. Digital forensics tools are used to collect and gather information on an electronic device while online investigation tools are used to gather, structure and use any information obtained on the web. The study notes Open-source intelligence (OSINT) as a main method in gathering

information online in cyber investigation. The study further highlights automation of IT tools and machine learning as new developments which speed up investigation process and achieve desired goals. The study is however limited since it only majors on digital forensic hardware and OSINT as an online investigation method exempting other crucial forensic tools of investigation. In research by Mohammed et al (2016) argued an automation-based approach to process Big Data particularly on digital forensic investigations.

The scholars discussed that processing and analyzing big data proves to be a challenge in itself, especially in a prevailing heterogeneous data of criminal cases (Mohammed et al., 2016). A study by Masombuka et al. (2018) propagated the techniques and methodologies for applying Artificial Intelligence (AI) to digital forensics investigations and purposes an active defense framework. The research aimed at exploring innovative methods of combatting cyberattacks in South Africa. AI applications enhance users to be cyber-resilient and improve cybersecurity performance. The study however bases its focus on AI leaving out other forensic tools which are essential in combatting cyberattacks. A similar study performed by Al Fahdi et al. (2016) argues that AI should be utilized in cybercrime profiling. The AI-powered software is utilized in phases of examination and analysis of digital forensics. Forensic experts are able to analyze and examine digital evidence across a variety of cybercrimes including spyware, hacking, malware, identity theft and data theft using this software. Hasan et al. (2011) coined a digital forensic model as a means of incident response. The scholars suggested integration of AI technologies to improve efficiency and effectiveness of the incident response system. The model however suffers limitation since the researchers did not share an experimental demonstration. This model's development and testing was not fully realized nor completed.

While there still exists robust studies on IT tools applied in cybercrime investigation, none conclusively highlights the application of IT, quality and quantity of evidence, and enhanced security of law enforcers to effective cybercrime investigation especially in a developing country like Kenya. Therefore, this study seeks to fill this gap.

2.5.2 ICT application on DCI

Cybercrime is increasingly becoming a major social problem in emerging economies. These crimes are on the increase in Kenya with statistics showing huge losses incurred annually due to high degree of digitization of economic activities (Cyoy, 2022). Expertise tools including GPS tracking, heat sensors, facial recognition, internet, data gathering systems, telecommunication systems, and surveillance cameras are essential in investigating, preventing, detecting, preventing and prosecuting crime in law enforcement (Suleiman et al., 2020). These emerging innovations in the technological era prompt DCI, Kenya to acquire and upgrade on existing tools and networks to fight cybercrime. IT bears the potentials to analyze cybercrime through use of technology to access data effectively addressing and mitigating it.

Among the foremost responsibilities bestowed upon the State, the highest obligation is the maintenance of public law and order, and the preservation of the rule of law. This stands as a cornerstone of effective governance, as the breakdown of public order and the rule of law can erode citizens' trust in their government and undermine its legitimacy. The role of Information and Communication Technologies (ICTs) becomes pivotal in reshaping the police force, transforming it from a coercive governmental entity into an agency primarily dedicated to safeguarding the lives and liberties of the general populace.

Nevertheless, the recent evolution of digital technology has engendered profound shifts in societal norms; particularly in how information is accessed, and interpersonal communication is

conducted. The behaviors, especially of the younger generation, have undergone significant transformations due to these technological advancements. While this progression has given rise to novel forms of criminal challenges, it has also facilitated the prevention, detection, investigation, prosecution, and punishment of these offenses. According to Hendricks (2013), the advent of information technology has endowed authoritarian states with the means to surveil, manage, and exert control over their subjects. However, this very technology, along with the human rights associated with it, has also worked to undermine their dominance. Harnessing these technologies extensively can enable the anticipation and thwarting of criminal activities before their actual occurrence, thus enhancing overall security.

The integration of ICT has become ubiquitous in daily life globally. Consequently, there is a strong belief that the resounding successes recorded by ICT across various domains substantiate its potential to significantly contribute to resolving the persistent challenge of insecurity in Kenya. The earliest instances of ICT adoption can be traced back to the military and security sectors during the Cold War in the 1940s. In the late nineteenth century, the usage of two-way radios, motor vehicles, and computers assisted in dispatching police work. Such applications for policing and national security included, but were not limited to, the Internet, DNA analysis techniques, biometric identification technologies, closed-circuit television (CCTV) and mobile phone cameras, eavesdropping devices, networked databases, and neural networks for data analysis, as well as voice recognition systems.

The foundation of scientific research facilitates the emergence of innovative technologies for the prevention of criminal activities. Hence, greater engagement of the scientific and technological community in crime reduction strategies is imperative. Crime detection, prevention, reduction, and control persist as pressing concerns due to the substantial threat posed by criminal

actions to society, especially as offenders embrace increasingly sophisticated technological tools for unlawful deeds. In accordance with Chika (2014), video and CCTV cameras stand as vital components and tools in employing ICT to counter and forestall criminal activities. Regrettably, some of these systems have fallen into disuse due to inadequate initial planning, insufficient monitoring, and instances of corruption in the award and execution of contracts. Numerous African countries have experimented with such crime detection methods but with limited success.

IT has drastically transformed police work and expectations of various police services. Therefore, to reap benefits of IT, organizations should recruit skilled and committed workers who will increase utilization of IT to address crime (Alberus, 2019). The way investigation occurs in for instance Australia has been revolutionized through the use of IT. They have been capable in reducing crimes through the use of predictive analysis and GPS maps which show hotspots of crime in the state (Suleiman et al., 2020). IT therefore proves to be a solution in addressing crime and assisting police to accurately keep track of crime statistics (Alberus, 2019).

2.6 Theories of the study

This study will be entrenched in three theories that are in line with the subject under investigation. The theories will be based at an individual level especially on the individual features that increase the chances of occurrence of a cybercrime.

2.6.1 Information Theory

The Information Theory, initially conceived by Willmer in 1970 and later expounded upon by Leeney in 2018, introduces a compelling analogy between criminal investigations and a battle of information. This theory underscores the critical role of information flow and its impact on the probability of law enforcement successfully identifying suspects in criminal cases. It posits that

the information emitted by criminals and the measures taken by law enforcement to collect and interpret that information are pivotal factors in determining the success of a criminal investigation (Rossmo, 2022). An essential element of this theory is the concept of "noise" in the investigative process, categorizing it into two forms: background noise and internal noise.

Background Noise signifies the dearth of information accessible to law enforcement during investigations (Rossmo, 2022). A lack of information obstructs their ability to comprehensively understand the signals emitted by criminals. Addressing background noise necessitates improvements in information gathering and intelligence-sharing mechanisms within law enforcement agencies. In contrast, Internal Noise arises from signal distortion, potentially caused by the deliberate dissemination of misinformation by criminals or errors in the information processing procedures of law enforcement (Leeney, 2018). Minimizing internal noise requires enhancing the accuracy and reliability of the information gathered and analyzed by law enforcement agencies. Information Theory emphasizes the dynamic relationship between offenders and law enforcement, categorizing information as active (emanating from criminals) or passive (gathered by law enforcers). The effectiveness of investigations hinges on the efficient exchange and utilization of information between these two parties. When criminals succeed in limiting information available to law enforcement, the likelihood of a successful investigation diminishes, thus increasing the odds of the criminal evading detection. Conversely, when law enforcers can collect and interpret information effectively, the probability of apprehending the criminal rises.

Despite the insights provided by Information Theory into the dynamics of criminal investigations, it bears certain limitations. The theory operates under the assumption of a simplified and idealized scenario where information flow between criminals and law enforcers is well-

defined and easily measurable, overlooking the complexities and uncertainties inherent in real-world investigations (Sager & Afzal, 2022). In practice, criminals can actively obfuscate or manipulate information, posing challenges for law enforcement's accurate interpretation and use of available data. Additionally, the theory may not fully account for the ever-evolving technological landscape and its impact on information exchange in criminal activities (Rossmo, 2021). With the rapid advancement of communication technologies and encryption methods, criminals can employ sophisticated means to conceal their activities, making it even more arduous for law enforcers to access vital information.

In the context of our study, Information Theory holds significant relevance. Our research aims to investigate the application of this theory in cybercrime and digital investigations, where criminals leave digital footprints, electronic evidence, and information trails. Simultaneously, cybercriminals may engage in techniques like mystification, encryption, and anonymization to distort or restrict available information. This theory underscores the importance of enhancing law enforcement's technological capabilities and knowledge to effectively collect, process, and interpret digital evidence. Moreover, it emphasizes the need for bolstered collaboration and information sharing among various law enforcement agencies, both at national and international levels, to address the transnational nature of cybercrime. A proactive and agile approach is advocated, which includes adopting advanced technologies and nurturing a skilled cybercrime investigative workforce to confront the evolving challenges posed by digital advancements.

2.6.2 Social Structure Social Learning Theory (SSSLT)

Social Structure Social Learning Theory (SSSLT) is a relatively recent theoretical framework developed by Akers and Jennings in 2016, focusing on the sociological aspects of crime assessment and predicting crime outcomes (Akers & Jennings, 2016). This theory comprises four

central components: imitation, differential reinforcement, differential association, and crime definitions. It is built upon the foundation of the Social Learning Theory (SLT) introduced by Burgess and Akers in 1966 (Opp, 2020).

In SSSLT, the element of imitation suggests that individuals are more likely to commit crimes if they observe others committing crimes and being rewarded for their actions. Differential reinforcement posits that the likelihood of crime increases when the expected rewards for criminal behavior outweigh the anticipated punishments. In simpler terms, if individuals consistently receive rewards for engaging in certain criminal activities, they are more likely to repeat those behaviors (Li et al., 2022). The concept of differential association in SSSLT states that individuals are more inclined to commit crimes if they spend a significant amount of time with peers engaged in criminal acts (Akers et al., 2016). Lastly, the theory of crime definitions in SSSLT explores how individuals justify and evaluate their desire to commit a crime, including assessing whether internalized norms prohibit the crime and evaluating the satisfaction of their needs through criminal behavior.

While Social Structure Social Learning Theory (SSSLT) offers valuable insights into the sociological aspects of crime and its prediction, it does have certain limitations. The theory heavily relies on the assumption that criminal behavior is primarily learned through social interactions and reinforcement processes, potentially oversimplifying the multifaceted nature of criminal behavior (Opp, 2020). Furthermore, the theory tends to generalize the learning process, overlooking individual variations and the influence of personal psychological traits or genetic predispositions, thus limiting its predictive power (Li et al., 2022). Additionally, the theory's emphasis on learning through associations and interactions may overlook the importance of individual agency and free

will, as people can resist or reject criminal behavior, even in the presence of conducive social structures.

In the context of our study, Social Structure Social Learning Theory (SSSLT) holds considerable relevance. Our research focuses on cybercrime, a domain where complex social interactions play a crucial role. Understanding the sociological factors influencing cybercriminal behaviors is essential for effective investigation and prevention strategies. SSSLT's element of imitation is particularly pertinent in cybercrime, where individuals may learn and replicate hacking techniques, fraud schemes, or other cybercriminal activities by observing others. Furthermore, the online environment fosters the formation of cybercriminal networks and communities, enabling knowledge sharing and interaction. The theory's focus on how individuals justify and evaluate criminal desires can provide insights into cybercriminal motivations and rationalizations. Understanding these factors can assist in designing targeted prevention and intervention programs that address the root causes of cybercriminal behaviors.

2.6.3 Routine Activity Theory

The Routine Activity Theory (RAT), initially formulated by Cohen and Felson in 1979 to elucidate changes in crime rates in the U.S. from 1947 to 1974, holds considerable relevance in the realm of cybercrime. It provides valuable insights into the factors contributing to cyber-related criminal activities (Guerra & Ingram, 2022). RAT posits that the likelihood of criminal victimization escalates when three elements converge: the absence of a capable guardian, the presence of a motivated criminal, and the existence of an attractive target (Wachs et al., 2021). In the context of cybercrime, these elements find application as follows:

1. Absence of Capable Guardian: In the digital sphere, a capable guardian pertains to security measures and protective mechanisms that shield against cyber threats. This encompasses

practices like employing antivirus software, regularly updating security settings and passwords, and exercising caution when using public computers. Neglecting these safeguards renders individuals or organizations more vulnerable to cyberattacks and data breaches.

2. Motivated Offenders: In the cyber landscape, motivated offenders encompass individuals or groups with malicious intent, engaging in cyber-harassment, creating and distributing viruses, conducting phishing attacks, and committing other cybercrimes. These offenders exploit vulnerabilities and weak security practices to perpetrate their illicit activities.

3. Attractive Targets: Cybercriminals actively seek out attractive targets offering potential gains with minimal risks. Online routine activities, such as emailing, online shopping, and banking, present appealing opportunities for cyber thieves involved in identity theft and financial fraud.

The application of RAT to cybercrime illuminates how the interplay of these elements influences the occurrence of various cyber threats. For instance, the absence of capable guardians, such as inadequate security measures and outdated software, provides opportunities for motivated offenders to launch cyber-harassment campaigns and distribute viruses, causing harm to individuals and organizations. Online routine activities like emailing, online shopping, and banking make individuals more susceptible to identity theft when attackers exploit security weaknesses or engage in phishing scams.

While RAT is relevant to the context of cybercrime, it does possess certain limitations. The theory predominantly concentrates on the immediate situational factors leading to criminal victimization, potentially overlooking the broader socio-economic and cultural contexts shaping cybercriminal behavior (Wachs et al., 2021). Cybercrime often stems from multifaceted motives, such as financial gain, political agendas, or ideological beliefs, which RAT may not fully account for. Additionally, RAT assumes a stable and predictable pattern of routines, which may not apply

in the rapidly evolving landscape of cyber activities. As technology advances, cybercriminals continuously adapt their methods, making it challenging to identify consistent routines and patterns in their activities. Furthermore, RAT's focus on the convergence of specific elements may disregard the potential interaction between various factors contributing to cybercrime (Guerra & Ingram, 2022). Human behavior, individual motivations, and societal influences are intricate and interconnected, making it difficult to isolate a single cause for cybercriminal activity.

In the context of our study, incorporating the Routine Activity Theory (RAT) enhances our understanding of the factors contributing to cybercrimes. This insight is crucial for developing effective strategies to combat cyber threats and enhance cybersecurity. It underscores the significance of proactive measures, security awareness, and individual responsibility in mitigating cyber risks. Policymakers can employ this theory to design targeted interventions and policies addressing the specific elements within RAT, thereby reducing the overall cybercrime risk and fortifying the protection of individuals and organizations in the digital age.

2.7 Variables influencing the application of IT tools

The application of IT by investigative agency on emerging cybercrime cases and intelligence gathering will promote effective cybercrime investigation within the DCI. The quality and quantity of evidence and information obtained due to the capacity to process and analyze huge amounts of information and finally filter it out guarantees a conviction. On the other hand, crime intelligence gathering by the DCI using virtual tools including crime mapping software as well as digital analytical tools which assist in collecting information as well as filter information which is helpful in effective cybercrime investigation.

Bougaardt and Kyobe (2011) in their study of factors inhibiting measurement losses of cybercrime, found quality of information system security design positively significant to losses of cybercrime. The study discovered that anti-virus software provides nature of attacks and frequency reports which is useful in determining damage extent. On the other hand, lack of knowledge on IT risks was found to be a major factor hindering small firms from effective monitoring of business operations,

Grigaliūnas and Toldinas (2020) propagate modelling digital evidence using habits attribution profiling and digital evidence object (DEO) method. The researchers discussed a systematic approach in dealing with the issue of profiling, habits and attribution using a feature diagram. The model emphasized on digital evidence investigation that applies attributed habits reducing the number of artefact search sequences from the set of digital user placates. The DEO model emphasizes on the analysis of information extracted from the forensic process using the elements of category theory considering the 5Ws (What, Who, Why, When and Where).

Deflem and Shutt (2008) in their study promulgate law enforcement as a major component to enhance computer security. The study shows a positive significant relationship between law enforcement and computer security. It discusses that prevailing notions of jurisdictional powers should be redefined to meet global needs of information security. On the other hand, the study recommends legislative efforts on cybercrime to be extended across global borders to mitigate cybercrimes and related cross-border threats against computer security.

Oksanen and Keipi (2013) study examined independent variables: age gender and experience to determine if young people are victims of internet crimes. Respondent's age was determined using age groups; gender was measured using female and male; and experience was

measured by the respondent's exposure to violence. The findings postulated young people as potential cybercrime victims even when other factors are adjusted.

2.8 Conceptual Framework

Theoretically, IT has been recognized as an important determinant to the success of a cybercrime investigation process. Additionally, it has been regarded as the backbone of a cybercrime investigation (Samoei, 2018). The use of IT in cybercrime investigation has contributed to ease of data transmission, process, storage and collection in form of data, text, images and voice (Francis, 2016).

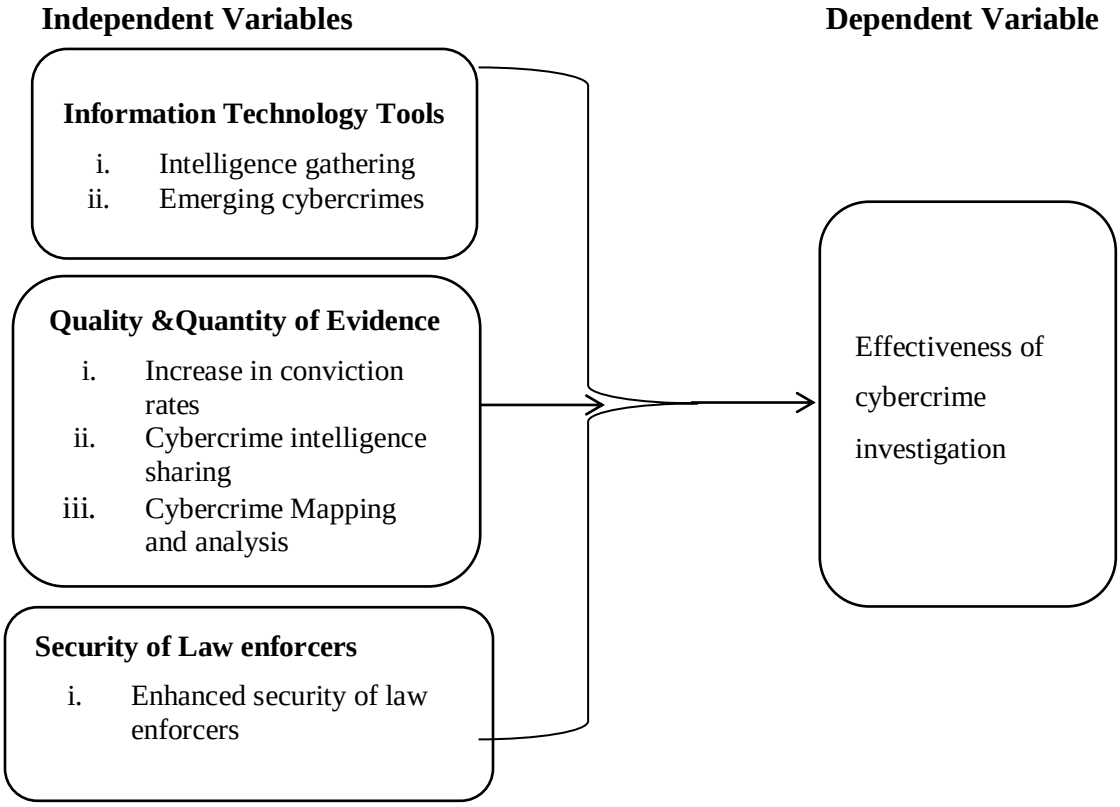

FIGURE 2. 3:

Conceptual Framework

The variables of this study will be operationalized as shown in Table 2.1

TABLE 2. 1:

Operationalization Of Variables

Variables	Sub-dimensions	Indicator	Values	Scale
Information Technology	i. Intelligence Gathering	-Application of automated programs and software -Forensic tools usage	-Software and programs -Forensic tools ownership	Nominal Ordinal
	ii. Emerging Cybercrimes	- Global computer networks -Increased number of security vulnerability	- Internet access at different places -Number of cyber threats reported in 2021	Ordinal Nominal
Quality and Quantity of Evidence	i. Increase in conviction rates	- Increase in number of attacks -Observed distributed pattern of attacks	-How many cyber-attacks occurred in 2021 compared to 2020 -Similarity in how the cybercrimes occur	Ordinal Nominal
	ii. Cybercrime intelligence sharing	-Aggressive activity against target networks -Domains and addresses that control access	-Network providers -Registered domains and addresses	Nominal Ordinal
	iii. Cybercrime mapping and analysis	-Risk assessment	-Scale of its consequences -Likelihood of future occurrence	Ordinal Nominal
Security of law enforcers	i. Enhanced security of law enforcement	-Arrests made on cyber-related crimes -Reported levels of cybercrime -Response time	-Number of cyber related crime arrests in 2021 -How many reported cybercrimes in 2021 compared to 2020 -Effective response on reported cybercrimes	Nominal Ordinal
Moderators	i. Age	-Age group	16-20, 21-30, 31-40….	Ordinal
	ii. Gender	-Female -Male	-F,M	Nominal
	iii. Experience	Number of years worked in DCI	<5, 5-10, 11-15, 16-20.....	Ordinal
Effectiveness of cybercrime investigation	i. Cyber security	-Effectiveness of cyber security measures -Detection speeds	- Number of cyber-security measures -How long cybercrime detection process takes	Nominal Ordinal
	ii. Cyber resilience	-Repeated staff training -Resourcing of cybersecurity tools	-Frequency of staff training - Period of changing cybersecurity tools	Ordinal Nominal

2.9 Chapter summary

Research has shown that cybercrime investigation is a revelatory process that law enforcers put collective efforts in building the truth through continuous collection and analysis of accessible information. Moreover, research has shown that cybercrime is a phenomenon that needs to be eradicated prompting investigators to adopt sophisticated modern IT tools to fight. Worth noting, none of the research in the literature review fully addresses the application of IT in cybercrime investigation. Furthermore, no study has tested the unified potentials of Routine Activity Theory, Information Theory, and Social Structure Social Learning Theory. It is against this gap that this study finds gravitas.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter focuses on outlining the methodologies employed in conducting the study, delving into the research design, sampling techniques, target population, and sample selection. It will also elaborate on the data collection tools and analysis methods utilized to evaluate the application of information technology in cybercrime investigation. Moreover, the reliability and validity of the data instruments will be thoroughly examined. A research methodology refers to the specific approaches adopted for data collection and analysis, crucial for conducting a research study. It serves as a roadmap guiding the researcher in establishing objectives and addressing research questions, culminating in the acquisition of relevant data during the study period (Sileyew, 2019). The selection of a particular methodology hinges on the nature of the subject under investigation and the study's objectives. Research itself is an organized endeavor aimed at acquiring knowledge and understanding about a particular subject (Asenahabi, 2019).

This chapter will clarify the complexities of the chosen research design, delineate the techniques employed in sampling, and specify the characteristics of the target population. Furthermore, it will expound on the data collection tools implemented to gather information pertinent to the investigation of cybercrime, and the subsequent analysis techniques applied to interpret and draw meaningful conclusions from the data. In doing so, the chapter will provide a comprehensive overview of the methodologies deployed, ensuring the reliability and validity of the study's findings.

3.2 Research design

Research design embodies the researcher's conceptual framework (Asenahabi, 2019), encompassing the overall structure of the study and the cohesive functioning of its key components in addressing the research inquiries. Its purpose is to establish a suitable framework for conducting the investigation (Sileyew, 2019). In this study, a descriptive correlational design was employed, chosen for its ability to assess the degree of association between variables, including information technology tools, the quality and quantity of evidence, law enforcement security, and the effectiveness of cybercrime investigation. This design facilitated a comprehensive understanding of the relationships between the identified factors, allowing for a nuanced exploration of their interconnections and impact on the phenomenon under study.

3.3 Study Area

The research took place in DCI, primarily because of the convenient access to IT resources and the fact that it serves as the central department responsible for conducting investigations related to serious crimes.

3.4 Study Population

The study's target population refers to the specific group of interest that the research aims to investigate (Majid, 2018). In this case, the research will be conducted in Nairobi, the largest city in Kenya, and focused on police officers working within the DCI (Directorate of Criminal Investigations) department. According to Sigilai (2018), the DCI department comprises a total of 6,043 police officers, who are distributed among different ranks, namely top, middle, and low.

The targeted population for this study was the 6,043 police officers serving in the DCI department within Nairobi County, encompassing individuals from all three ranks – top, middle, and low. These officers played pivotal roles in conducting criminal investigations and maintaining law and order in the region. The research seeked to examine and gain insights into various aspects related to cybercrime investigation, and by focusing on this specific group of police officers, it aimed at gathering valuable firsthand information from professionals actively involved in combating cyber-related criminal activities. Their experiences, expertise, and perspectives will contribute significantly to the study's depth and accuracy.The diagram below provides a breakdown of the number of police officers within each rank in the DCI department:

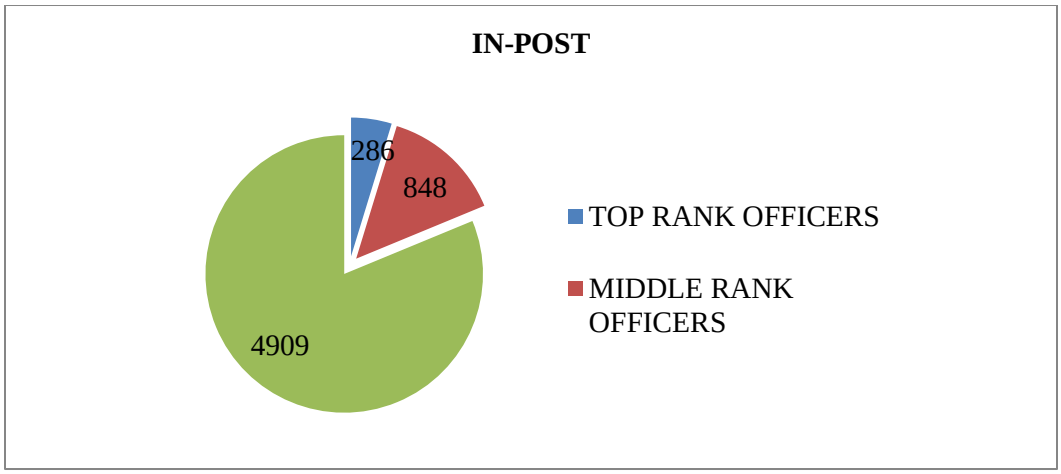

Figure 3. 1: Target Population in DCI

Source: Sigilai (2018)

By concentrating on this well-defined target population, the study ensured that the findings obtained are relevant and applicable to the specific context of cybercrime investigation in Nairobi County and can potentially inform and enhance law enforcement strategies and practices in the area.

3.5 Sample of the study

The study consisted of a sample size of 361 police officers, who were randomly chosen from the Directorate of Criminal Investigations department. The selection was drowned from multiple integral DCI units known for their significant reliance on information technology, including the Cybercrime Unit, Anti-Banking Fraud Unit, Forensics Unit, Ballistics Unit, and Special Crime Prevention Unit.

As the total population size is already known, the study will employ Thakur's (2022) sample size formula to determine the appropriate sample size for the research. This formula enabled the researchers to estimate the number of participants needed to represent the larger population adequately. By using a random sampling method and selecting officers from diverse units within the DCI, the study aimed at obtaining a representative sample that can provide valuable insights into the application of information technology in various aspects of cybercrime investigation. This approach ensures the findings can be generalized to the broader population and enhances the study's overall validity and reliability.

$$\text{Sample size, } n = N * \frac{\frac{Z^2 * p * (1-p)}{e^2}}{[N - 1 + \frac{Z^2 * p * (1-p)}{e^2}]}$$

Where;

N= Size of the population

Z= Normal distribution's critical value at 95% confidence level (1.96)

P=Proportion of sample

e=Error margin (0.05)

n= $6043*(1.96^2*0.5*(1-0.5)/(0.05^2))/(6043-1+(1.96^2*0.5*(1-0.5))/(0.05^2)$

n=361.25~361

The police officers were sampled according to their ranks as shown in the table below;

Table 3. 1: Distribution of Samples

Category	**Population (N)**	**Percentage**	**Sample distribution**
Top Ranking Officers	286	4.7%	17
Middle Ranking Officers	848	14.1%	51
Low Ranking Officers	4909	81.2%	293
Total	**6043**	**100%**	**361**

Source: Own Conceptualization

3.6 Sampling design

As stated by Lohr (2021), sampling design encompasses the statistical principles involved in the selection of samples and the subsequent analysis of data gathered from a sample survey. For this study, the chosen sampling design was random sampling, which involves the random selection of participants from the DCI department to collect data. The rationale behind opting for simple random sampling is the homogeneity observed within the target population. By using this method, questionnaires were distributed randomly to participants of various ranks, ages, genders, and locations within the study area.

This approach ensures that each individual within the DCI department has an equal chance of being included in the sample, thus reducing the potential for bias and producing a representative subset of the population. By collecting data from a diverse range of participants, the study obtained comprehensive insights into the application of information technology in cybercrime investigation across various groups within the DCI, enhancing the overall validity and reliability of the research findings.

3.7 Data collection

This study adopted primary and secondary data collected through the qualitative and quantitative data methods and literature review. Questionnaires and interview questions were prepared to collect data required for the study. Data was collected across 8 units in the DCI department while respondents being police officers of different ranks. Secondary data were sourced from journals, articles and textbooks. The information and facts obtained through interviewing signifies a respondent's opinion, thoughts and feelings hence their participation is critical. According to Moser and Korstjens (2018), the researcher should encourage respondents to speak freely through establishing a good rapport.

3.7.1: Validity of the Instrument

Validity sole purpose is an appropriate and meaningful data from the evaluating tool used in analysis (Sürücü & Maslakçi, 2020). Validity is whether the evaluating tool measures what it is intended to measure. To ensure that this study was conducted with valid measurements, questionnaires were pre-tested to obtain content validity. Content validity is a validity that divulges in the extent to which each measuring tool such as questionnaire serves its purpose (Yusoff, 2019). This was done through pre-testing of the questions to refine the clarity. According to Kothari (2014), research's tool validity is how well it evaluates what it is required to evaluate. An instrument content validity was established through peer review and analysis by research experts, involving my supervisor to confirm whether questionnaires' content was suitable and significant for the study. In checking the content and format of the instrument, experts' opinion was sought.

3.7.2: Reliability of the Instrument

Borg and Gall (2016), defines reliability as an indicator of whereby a researcher realizes constant results as a result of several trials. Borg and Gall state that content reliability of an instrument improves through expert views. Kothari (2014) states reliability as the extent towards

a research tool yields steady outcomes when recurrent trials are taken. This implies that the research instrument should produce same outcomes if repeatedly administered. To ensure reliability, this study adopted internal consistency technique. Mugenda and Mugenda (2003) in their study indicate that, a one item score is correlated with other items scores in the research instrument in this approach. To establish how the items, associate, the study utilized SPSS to calculate the Cronbach's coefficient alpha.

Uma (2006) indicates that a reliability coefficient close to 1.0 is considered better while reliabilities less than 0.60 is considered poor. Reliabilities in the range of 0.70 is acceptable, while those above 0.80 is good.

According to Sürücü and Maslakçi (2020), reliability is the consistency of a measuring instrument when used over time. Measuring instrument' reliability is essential for healthy results of the study. This study increased its reliability using Cronbach Alpha.

3.8 Data Analysis

Data analysis involves various phases; interpreting, describing, evaluating significance and drawing conclusions (Schoch, 2020). This study examined the application of IT in cybercrime investigation in DCI, Kenya. Both quantitative and qualitative data were organized, described, coded, and analyzed. Quantitative data based on percentages and statistics was analyzed using the statistical analysis software package known as Statistical Package for the Social Sciences (SPSS). Moreover, qualitative data was analyzed using content analysis to assess the application of IT in cybercrime investigation in Kenya with a lens on the DCI. The model was tested using data collected from 361 police officers employed under DCI department.

The model fitness was validated using cross-validation; the model's predictive power is assessed using some of the data while the remaining data is utilized to estimate the model's coefficients. The analysis showed how much of the total variance in the dependent variable (effectiveness of ICT tools) is possible to explain by the independent variables; To determine the statistical significance of the correlations between the independent variables, Analysis of Variance (ANOVA) was conducted. The level of association between the dependent and independent variables in the model are indicated by p-value of the F-test. When the significance p-value is less than 0.05, it shows a statistically significant relationship between the dependent and independent variables. A p-value of 0.10 shows a weak significant relationship. Pearson product-moment correlation was utilized to find how much the dependent variable, selected independent variables correlate with the acceptance of the model and their relationships.

3.8.1 Analytical model

In this study, the inferential statistics involved the use of multiple linear regression, while descriptive statistics encompassed frequencies and percentages. Through multiple linear regression, the research established and quantified the relationships between the dependent variable and multiple independent variables, providing valuable insights into the factors influencing the phenomenon under investigation. This analysis enabled the researchers to determine the strength and significance of these relationships, offering a deeper understanding of how the independent variables collectively contribute to explaining the variations in the dependent variable.

On the other hand, descriptive statistics, such as frequencies and percentages, were employed to summarize and present the characteristics and patterns observed in the data. This

helped in providing a clear and concise overview of the study's participants and key variables, facilitating a comprehensive understanding of the data distribution and aiding in the communication of research findings effectively. Together, these statistical approaches contributed to a robust and comprehensive analysis of the research data, supporting the study's objectives and enhancing the overall validity and reliability of the results.

The multiple linear regression model is as follows;

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

where;

Y= Effectiveness of cybercrime investigation

α= y intercept of equation

β_1 , β_2 $and \beta_3$ are the coefficients of regression

X_1= Information Technology Tools measured by Intelligence gathering and Emerging cybercrimes

X_2= Quality &Quantity of Evidence measured by Increase in conviction rates, Cybercrime intelligence sharing and Cybercrime Mapping and analysis

X_3= Security of law enforcers measured by Enhanced security of law enforcers

ε= term of error

3.8.2 Diagnostic Tests

In this study, the diagnostic tests employed encompassed various aspects, including autocorrelation testing, normality testing, multicollinearity testing, homoscedasticity testing, and linearity testing.

3.8.2.1 Autocorrelation Testing

Autocorrelation occurs when there is a correlation or association among the error terms in the observations. To examine the presence of autocorrelation, the study employed the Durbin-

Watson test statistic. This statistic usually takes values between 0 and 4. When the Durbin-Watson value falls within the range of 2 to 2.5, it indicates the absence of autocorrelation.

3.8.2.2 Normality Testing

In this study, the researchers investigated the distribution of residuals using a standard residuals P-P plot to assess its normality. When the residuals conform more closely to a normal distribution, the dots on the plot will cluster nearer to the diagonal line, indicating that the normality condition has been met. Conversely, if the dots deviate significantly from the diagonal line, it suggests that the residuals are not normally distributed, indicating a failure to meet the normality condition (Khan et al., 2022).

3.8.2.3 Multicollinearity Testing

Shrestha (2020) defines multicollinearity as a situation where independent variables exhibit a relationship, leading to an increase in the standard error of coefficients. This inflation of standard errors can result in certain variables being statistically insignificant, even though they should be significant in reality. The accuracy of estimating regression parameters decreases as two variables become more multicollinear.

In the study conducted by Onyango (2022), the Variance Inflation Factor (VIF) was utilized to detect multicollinearity. A VIF value greater than 10 indicates the presence of multicollinearity, while a VIF value less than 10 suggests a lower amount or absence of multicollinearity.

3.8.2.4 Homoscedasticity Testing

One of the fundamental assumptions in linear regression is homoscedasticity, which refers to the constant variance of the errors or residuals (Đalić & Terzić, 2021). However, in cases

where this assumption is violated, heteroscedasticity arises. To identify the presence of heteroscedasticity in this study, the graphical method was used.

3.8.2.5 Linearity Testing

Testing for linearity is crucial because numerous statistical techniques rely on the assumption that the data follows a linear pattern. To assess linearity, a significance test is performed. If the significance level (sig. deviation from linearity) is greater than 0.05, it indicates that the relationship between the independent variables is linearly dependent. This means that the data shows evidence of following a linear pattern.

On the other hand, if the significance level (sig. deviation) is less than 0.05, it suggests that the relationship between the independent variables is not linearly dependent. This means that, the data does not conform to a straight-line relationship.

3.9 Ethical Considerations

This study ensured that no plagiarism took place while using the secondary data sources. Similarly, the data or information that was collected in this study was solely used for academic purposes. Finally, the data obtained from respondents was treated with ultimate confidentiality and allowed to voluntarily participate.

CHAPTER FOUR

DATA ANALYSIS, FINDINGS, AND DISCUSSION

This chapter aims to interpret, elucidate, and analyze the data findings obtained in this study. The information is presented in sections providing insights into the reliability and validity of the data, the rate at which the questionnaire was completed by respondents, the characteristics of the participants, as well as statistical analyses involving both descriptive and inferential statistics. Additionally, diagnostic tests will be conducted to ensure the quality and accuracy of the data. The results of these analyses will be presented in the form of tables and figures, allowing for a comprehensive understanding of the study's findings.

4.1 Validity and Reliability of Instrument

The study aimed to assess the validity and reliability of the research instrument. The results are presented in Table 4.1 and Table 4.2. Table 4.1 includes the items ITT (Information Technology Tools), QQE (Quantity and Quality of Evidence), SLE (Security of Law Enforcers), and ECI (Effective Cybercrime Investigation).

TABLE 4.1

Validity Results

TABLE 4. 1: Correlations

		ITT	QQE	SLE	ECI
ITT	Pearson Correlation	1			
	Sig. (2-tailed)				
	N	351			
QQE	Pearson Correlation	.683**	1		
	Sig. (2-tailed)	.000			
	N	351	351		
SLE	Pearson Correlation	.303**	.541**	1	
	Sig. (2-tailed)	.000	.000		
	N	351	351	351	
ECI	Pearson Correlation	.610**	.723**	.443**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	351	351	351	351

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

Based on the findings presented in Table 4.1, it can be concluded that items ITT, QQE, SLE and ECI have significance levels of .000, which is also lower than the standard significance level of 0.05, suggesting its validity. Hence, it can be concluded that items ITT, QQE, SLE and ECI are valid.

Table 4. 2

Reliability Statistics

Cronbach's Alpha	N of Items
.811	21

According to Uma's study conducted in 2006, the data collection instrument demonstrates reliability, as indicated by a Cronbach's alpha value of 0.811, which exceeds the threshold of 0.6.

4.2 Questionnaire Response Rate

The study distributed a total of 361 questionnaires, out of which 351 were accurately and fully completed and subsequently collected. This results in a return rate of 97.2%, as indicated in Table 4.3. According to Onyango's (2022) assessment, a return rate of 97.2% is regarded as excellent.

TABLE 4. 3

Response Rate

Reaction	Frequency	Percent
Accurately and completely filled	351	97.2%
Unanswered	10	2.8%
Total	**361**	**100%**

4.3 Demographics

The study encompasses various demographic characteristics of the participants, such as gender, age group, department, years of experience, rank held, and education level within the police department. These specific attributes are presented in Tables 4.4, 4.5, 4.6, 4.7, 4.8, and 4.9 respectively.

4.3.1 Gender Distribution

Table 4.4 demonstrates a significant gender disparity within the DCI department, revealing that the majority of individuals occupying positions are male. Specifically, males comprise 80.1% of the workforce, while females represent only 19.9%.

TABLE 4. 4
Gender Distribution

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	281	80.1	80.1	80.1
	Female	70	19.9	19.9	100.0
	Total	351	100.0	100.0	

4.3.2 Age Distribution

Table 4.5 illustrates the age distribution of the respondents, with the highest percentage (31.3%) falling within the 31-40 years' age group. The second highest representation (27.1%) was observed among respondents aged 41-50 years. Those between 21-30 years accounted for 17.4%, while individuals over 51 years constituted 15.1% of the sample. Finally, respondents aged 16-20 years represented 9.1% of the total. These findings indicate that the majority of police officers were in the middle-aged range.

TABLE 4. 5
Age Distribution

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	16-20	32	9.1	9.1	9.1
	21-30	61	17.4	17.4	26.5
	31-40	110	31.3	31.3	57.8
	41-50	95	27.1	27.1	84.9
	Over 51	53	15.1	15.1	100.0
	Total	351	100.0	100.0	

4.3.3 Respondents per Department

Table 4.6 presents the distribution of respondents across various units within the DCI department. The data reveals that 4.3% of the respondents were affiliated with the Land Fraud Unit, while the Anti-Banking Fraud Unit accounted for 11.7%. The Special Crime Prevention Unit comprised 15.4% of the respondents, followed by the Cyber Crime Unit with 30.8%. The Anti-Narcotics Unit represented 13.1%, while the Forensic Department constituted 9.4%. The Serious Crime Unit accounted for 11.4% of the respondents, and the Ballistics Unit was represented by 4%.

TABLE 4. 6

DCI Departments

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Land Fraud Unit	15	4.3	4.3	4.3
	Anti-Banking Fraud	41	11.7	11.7	16.0
	Special Crime Prevention Unit	54	15.4	15.4	31.3
	Cyber Crime Unit	108	30.8	30.8	62.1
	Anti-Narcotics Unit	46	13.1	13.1	75.2
	Forensic Department	33	9.4	9.4	84.6
	Serious Crime Unit	40	11.4	11.4	96.0
	Ballistics Unit	14	4.0	4.0	100.0
	Total	351	100.0	100.0	

4.3.4 Respondents Years of Experience

Table 4.7 displays the distribution of respondents based on their years of experience working in the DCI (Directorate of Criminal Investigations). The data indicates that the majority of respondents (26.8%) had a tenure of 5-10 years in the DCI. Following closely, 23.9% of respondents had 11-15 years of experience, potentially indicating their strong sense of loyalty towards the organization. Additionally, 21.4% of police officers had served for 16-20 years, while 16.5% had less than 5 years of experience. Furthermore, 11.4% of respondents had an extensive tenure of over 20 years within the DCI.

TABLE 4. 7

Years of Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 5	58	16.5	16.5	16.5
	5-10	94	26.8	26.8	43.3
	11-15	84	23.9	23.9	67.2
	16-20	75	21.4	21.4	88.6
	over 20	40	11.4	11.4	41.4
	Total	351	100.0	100.0	100.0

4.3.5 Officers' Rank

Table 4.8 displays the distribution of respondents based on the ranks they hold within the DCI department. Most respondents were from bottom level rank represented by 45.6%, closely followed by middle level rank' respondents represented by 39.6%, and further respondents from top level represented 14.8%.

TABLE 4. 8

Rank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Top level	52	14.8	14.8	14.8
	Middle level	139	39.6	39.6	54.4
	Bottom level	160	45.6	45.6	100.0
	Total	351	100.0	100.0	

4.3.6 Education Level

Table 4.9 outlines the distribution of educational levels among respondents in the DCI department. The findings demonstrate that a significant proportion of respondents, specifically 47.9%, held a secondary education qualification. This prevalence could be attributed to the recruitment criteria typically required for police officers. The second most common educational

level among respondents was a diploma, accounting for 19.9%. Degree holders represented 14.8% of the sample, while certificate holders comprised 14%. A smaller proportion, 2.8%, held postgraduate degrees, and a mere 0.6% had a basic primary education. These results suggest that a considerable number of police officers have a substantial educational background.

TABLE 4. 9

Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Primary	2	.6	.6	.6
	Secondary	168	47.9	47.9	48.4
	Certificate	49	14.0	14.0	62.4
	Diploma	70	19.9	19.9	82.3
	Degree	52	14.8	14.8	97.2
	Postgraduate degree	10	2.8	2.8	100.0
	Total	351	100.0	100.0	

4.5 Descriptive Statistics

The study conducted descriptive statistical analysis with the findings outlined below in different sections.

4.5.1 Impact of Information Technology Tool

The objective of the study was to develop a regression model for cybercrime investigation within the Directorate of Criminal Investigations (DCI) in Kenya. Specifically, it aimed to examine the influence of information technology tools on the effectiveness of cybercrime investigation. The respondents were asked to rate various aspects of information technology tools' impact on effective cybercrime investigation using a 5-point Likert scale. Descriptive results of the assessment on Information Technology Tools are presented in Table 4.10.

TABLE 4. 10
Information Technology Tools

	N	Minimum	Maximum	Mean	Std. Deviation
To what extent has automated software and programs enhanced investigations through intelligence gathering among police Officers?	351	1	5	3.64	1.026
To what extent do you agree that cybercrime is reported frequently?	351	1	5	3.63	.997
To what extent do you agree that there's internet connectivity in your offices within Nairobi County?	351	1	5	3.54	1.073
Valid N (listwise)	351				

The table displays mean scores of above 3, indicating that most respondents agreed with the statements regarding information technology tools. Most respondents highly agreed that automated software and programs enhance investigations through intelligence gathering among police officers with mean score (3.64). Conversely, most respondents had a low agreement that offices within Nairobi County are connected to the internet with mean score of 3.54. On the other hand, most respondents recorded the highest variation of responses on offices within Nairobi County being connected to internet with a standard deviation of 1.073. Moreover, the frequency of reporting cybercrime exhibited the lowest response variation, with a standard deviation of 0.997.

4.5.2 Impact of Quality and Quantity of Evidence

The primary objective of the research was to develop a regression model for cybercrime investigation within the Directorate of Criminal Investigations (DCI) in Kenya. Specifically, the study sought to examine the impact of quality and quantity of evidence on the effectiveness of cybercrime investigation. The respondents were asked to evaluate the influence of various aspects

of quality and quantity evidence on effective cybercrime investigation using a 5-point Likert scale. The descriptive results of the assessment on quality and quantity evidence are presented in Table 4.11.

TABLE 4. 11
Quality and Quantity of Evidence

	N	Minimum	Maximum	Mean	Std. Deviation
To what extent do you agree that vulnerable internet service providers can compromise evidence collection?	351	1	5	3.70	1.026
To what extent do you agree that registering domains and addresses can secure intelligence sharing?	351	1	5	3.69	1.102
To what extent is the similarity in pattern of cybercrimes?	351	1	5	3.64	1.001
To what extent do you agree that cybercrime impacts huge losses on the economy?	351	1	5	3.49	.959
To what extent do you think cybercrimes will continue to rise?	351	1	5	3.46	.918
To what extent do you agree that there's increased number of cyber-attacks?	351	1	5	3.21	1.138
Valid N (listwise)	351				

Table 4.11 presents that most respondents had the highest level of agreement that vulnerable internet service providers can compromise evidence collection indicated by a mean score (3.70). On the other hand, the respondents had the lowest agreement that that there's increased number of cyber-attacks indicated by a mean score of 3.21. On the other hand, most respondents recorded a high variation in responses that there's increased number of cyber-attacks indicated by a standard deviation of 1.138. The lowest response variation on cybercrimes continuing to rise was indicated by a standard deviation of 0.918.

4.5.3 Extent of Security of Law Enforcers

The research aimed to establish the impact of security of law enforcers to effective cybercrime investigation. The respondents were to react to influence of numerous aspects of law enforcers security towards effective cybercrime investigation on a 5-points Likert scale. The descriptive results of the assessment on the security of law enforcers are presented in Table 4.12.

TABLE 4. 12
Security of Law Enforcers Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
To what extent do you agree that arrests are made in relation to cases of cybercrime?	351	1	5	3.56	1.042
To what extent do you agree that there's effective response to any reported crime with the use of current forensic tools you own?	351	1	5	3.09	1.268
Valid N (listwise)	351				

The results pertaining to the respondents' agreement regarding the security of law enforcers are presented in Table 4.12. The majority of participants expressed the highest level of agreement concerning making arrests in connection with cybercrime cases, with an average score of 3.56. On the other hand, the lowest level of agreement, with a mean of 3.09, was observed regarding the effectiveness of responses to reported crimes using currently owned forensic tools.

Conversely, the participants exhibited a high variability in their responses concerning the effectiveness of currently owned forensic tools in addressing reported crimes, with a standard deviation of 1.268. The lowest variation in responses, with a standard deviation of 1.042, was observed in the context of making arrests related to cybercrime cases.

4.5.4 Effectiveness of cybercrime investigation

The research aimed to establish a regression model adopted in cybercrime investigation within the DCI, Kenya. The respondents reacted to influence of numerous aspects of effective cybercrime investigation on a 5-point Likert scale. Table 4.13 outlines the results of the descriptive.

TABLE 4. 13
Effective cybercrime investigation Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
To what extent do you agree that information technology tools increase the detection of cybercrime?	351	1	5	3.84	1.105
To what extent do you agree that cybersecurity measures increase effective cybercrime investigation?	351	1	5	3.75	1.049
To what extent do you agree that continuous training of staff on how to use the forensic tools increases effective cybercrime investigation?	351	1	5	3.46	1.046
To what extent do you agree that there's continuous upgrade of cybersecurity tools within DCI?	351	1	5	3.46	.967
Valid N (listwise)	351				

Table 4.13 presents the results related to respondents' level of agreement with statements concerning effective cybercrime investigation. Most participants expressed the highest level of agreement with the statement indicating that information technology tools enhance cybercrime detection, which received the highest mean score of 3.84. Conversely, most respondents showed a lower level of agreement regarding the continuous upgrading of cybersecurity tools within the DCI, as evidenced by a mean score of 3.46. Additionally, there was a notable variation in responses among participants regarding the impact of information technology tools on cybercrime detection,

with a standard deviation of 1.105. However, there was relatively less variation in responses concerning the continuous upgrading of cybersecurity tools within the DCI, with a standard deviation of 0.967.

4.6 Inferential Statistics

In this section, the study conducted an analysis to examine the correlation between the independent variables and effective cybercrime investigation.

4.6.1 Correlation Analysis

To establish the non-causal association between the independent variables, including Information Technology tools (ITT), Quantity and Quality Evidence (QQE), and Security of law enforcers (SLE), as well as the dependent variable, Effective cybercrime investigation (ECI), the study employed Pearson product-moment correlation analysis. The results of this analysis are presented in Table 4.14 displaying the correlation between ITT, QQE, SLE, and ECI.

TABLE 4. 14
Correlations

		ITT	QQE	SLE	ECI
ITT	Pearson Correlation	1			
	Sig. (2-tailed)				
	N	351			
QQE	Pearson Correlation	.683**	1		
	Sig. (2-tailed)	.000			
	N	351	351		
SLE	Pearson Correlation	.303**	.541**	1	
	Sig. (2-tailed)	.000	.000		
	N	351	351	351	
ECI	Pearson Correlation	.610**	.723**	.443**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	351	351	351	351

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

The variable Information Technology Tools exhibited a significant moderate positive correlation with ECI, as evidenced by a sig-level of 0.000 and a Pearson Correlation coefficient of 0.610 under the significance level 0.01 in a 2-tailed test. These results are consistent with the findings of Wekundah's study conducted in 2015, which suggested that the utilization of systems and technology-based models increases the likelihood of effective cybercrime investigation. Likewise, Sigilai's (2018) study also supports these results, highlighting a positive association between information technology tools and effective cybercrime investigation. The research posited that information technology tools have facilitated the identification of valuable information from a pool of data, thereby enhancing crime intelligence effectiveness.

Moreover, the variable Quality and Quantity of Evidence exhibited a statistically significant high positive relationship indicated by a sig-value of 0.000 and Pearson correlation value of 0.723 in a 2-tailed test. These findings align with the conclusions drawn by Grigaliūnas and Toldinas in their 2020 study, which emphasized the utility of technology-based models in analyzing information derived from the forensic process, contributing to overall effective cybercrime investigation. Similarly, a study by Hasan et al. in 2011 supports these findings, highlighting that artificial intelligence models aid in expediting cybercrime investigation through intelligence gathering.

Similarly, the variable Security of Law Enforcers demonstrated a significant low positive correlation with Effectiveness of Cybercrime Investigation, as evidenced by a sig value of 0.000 and a Pearson correlation coefficient of 0.443. These results align with the findings of Deflem and Shutt's study in 2018, which recognize the significance of law enforcers' jurisdictional powers in ensuring information security. Their research emphasizes the importance of effective coordination and cooperation among law enforcement agencies to address cybercrime effectively.

4.6.2 Multiple Regression Analysis

In understanding individual relationships, a multiple regression analysis was undertaken. The output displayed in Tables 4.15, 4.16, and 4.17.

TABLE 4. 15

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.744[a]	.554	.550	.51174

a. Predictors: (Constant), SECURITY_OF_LAW_ENFORCERS, INFORMATION_TECHNOLOGY_TOOLS, QUALITY_QUANTITY_OF_EVIDENCE

The model summary reveals that the three variables (Security of Law Enforcers, Information Technology Tools, and Quality and Quantity of Evidence) collectively contributed to a coefficient of determination (R_2) of 0.554. This R_2 value indicates that the model successfully accounted for approximately 55.4% of the variances observed in effective cybercrime investigation, indicating a reasonably good fit. The remaining 44.6% of variations can be attributed to factors beyond the scope of this study.

TABLE 4. 16
ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	112.855	3	37.618	143.647	.000[b]
	Residual	90.872	347	.262		
	Total	203.727	350			

a. Dependent Variable : EFFECTIVE_CYBERCRIME_INVESTIGATION

b. Predictors: (Constant), SECURITY_OF_LAW_ENFORCERS, INFORMATION_TECHNOLOGY_TOOLS, QUALITY_QUANTITY_OF_EVIDENCE

The ANOVA findings pertaining to the model have been extracted and presented in Table 4.16. According to the table, the model demonstrated a highly significant sig-value of 0.000. This outcome strongly implies that the model, encompassing Security of Law Enforcers, Information

Technology Tools, and Quality and Quantity of Evidence as independent variables, holds substantial statistical importance in elucidating the linear association among these three predictors and effective cybercrime investigation.

TABLE 4. 17
Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.616	.149		4.137	.000	.323	.909
	ITT	.213	.046	.230	4.663	.000	.123	.303
	QQE	.560	.061	.513	9.176	.000	.440	.680
	SLE	.080	.036	.096	2.246	.025	.010	.151

a. Dependent Variable: EFFECTIVE_CYBERCRIME_INVESTIGATION

According to the Coefficients Table 4.17, the variable Information Technology Tools displayed a highly significant coefficient with a p-value of 0.000 in the combined model. This finding indicates a strong and meaningful association between this variable and effective cybercrime investigation.

Likewise, the quality and quantity of evidence also exhibited a significant coefficient with a p-value of 0.000, suggesting a notable correlation with effective cybercrime investigation.

Furthermore, an analysis of law enforcers' security revealed a remarkably low p-value of 0.025, signifying a substantial relationship with effective cybercrime investigation.

According to the findings, it can be formally inferred that the Security of Law Enforcers, Information Technology Tools, and the Quality and Quantity of Evidence exert a statistically

substantial influence on the effective cybercrime investigations in Kenya, particularly within the Nairobi DCI.

The multiple linear regression model was as follows;

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

where; Y= Effectiveness of cybercrime investigation, X_1= Information Technology Tools, X_2= Quality &Quantity of Evidence, X_3= Security of law enforcers, ε= term of error

The fitted equation is;

$Y= 0.616 + 0.213X_1 + 0.560X_2 + 0.080X_3$

According to the derived equation, denoted as Y, which represents the Effectiveness of cybercrime investigation, several factors contribute to its determination. These factors are represented as follows: 0.616 is a constant, indicating the level of effective cybercrime investigation in the absence of Information and Communication Technology (ICT) tools usage. Additionally, X_1 refers to Information Technology Tools, X_2 represents Quality and Quantity of Evidence, and X_3 corresponds to the Security of law enforcers.

The results of the investigation suggest that without the utilization of ICT tools, the effectiveness of cybercrime investigation would be at 61.6%. Among the factors considered, Quality and Quantity of Evidence exhibited the most significant impact on the effectiveness of cybercrime investigation. A one-unit change in this factor resulted in a considerable positive change of 56% in the effectiveness of cybercrime investigation.

Following closely, the use of Information Technology Tools exerted the second highest influence on the effectiveness of cybercrime investigation. A one-unit change in Information Technology Tools led to a notable 21.3% positive change in the effectiveness of cybercrime investigation.

Lastly, the Security of law enforcers had the least influence on the effectiveness of cybercrime investigation. A one-unit change in this factor corresponded to an 8% positive change in the effectiveness of cybercrime investigation.

In summary, these findings indicate that the usage of ICT tools had a positive and significant influence on the effectiveness of cybercrime investigation. Additionally, the study highlights the crucial roles played by Quality and Quantity of Evidence, Information Technology Tools, and Security of law enforcers playing significant roles in shaping this relationship.

4.7 Diagnostic Tests

In this study, the diagnostic tests employed encompassed various aspects, including autocorrelation testing, normality testing, multicollinearity testing, homoscedasticity testing, and linearity testing.

4.7.1 Autocorrelation Testing

In order to assess the existence of autocorrelation, the research utilized the Durbin-Watson test statistic

TABLE 4. 18
Autocorrelation Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.744[a]	.554	.550	.51174	1.673

a. Predictors: (Constant), SECURITY_OF_LAW_ENFORCERS, INFORMATION_TECHNOLOGY_TOOLS, QUALITY_QUANTITY_OF_EVIDENCE
b. Dependent Variable: EFFECTIVE_CYBERCRIME_INVESTIGATION

The value of the Durbin-Watson test statistic obtained from table 4.18 was 1.673, indicating presence of autocorrelation among the constructs.

4.7.2 Normality Testing

In this study, the researchers investigated the distribution of residuals using a standard residuals P-P plot to assess its normality.

Based on the observations made from Figure 4.1, 4.2, 4.3, and 4.4, it can be deduced that the residuals exhibit a stronger adherence to a normal distribution. The data points on the plots tend to cluster closer to the diagonal line, indicating that the normality assumption has been satisfied.

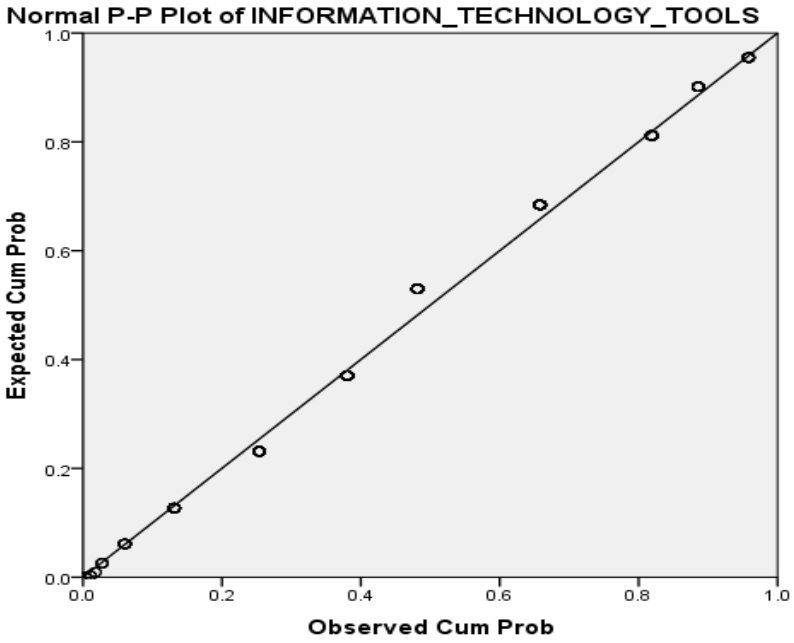

FIGURE 4. 1: ITT Normality Test

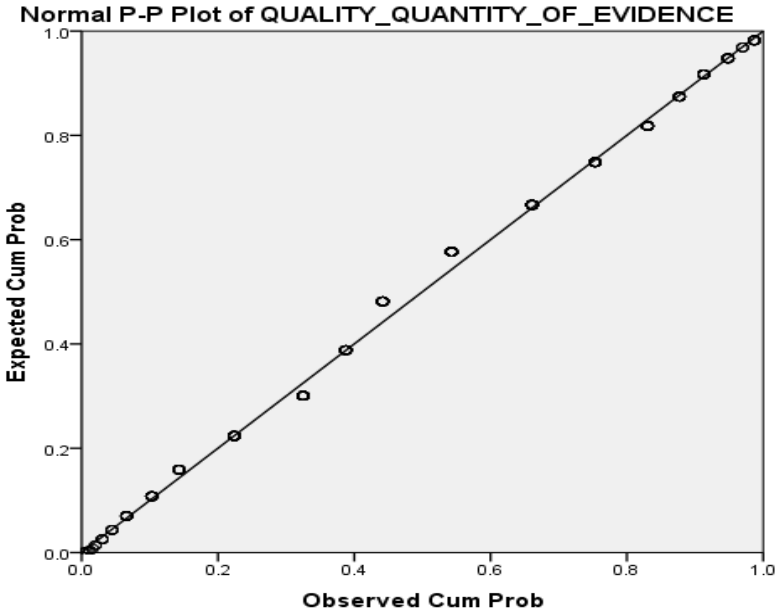

FIGURE 4. 2: QQE Normality Test

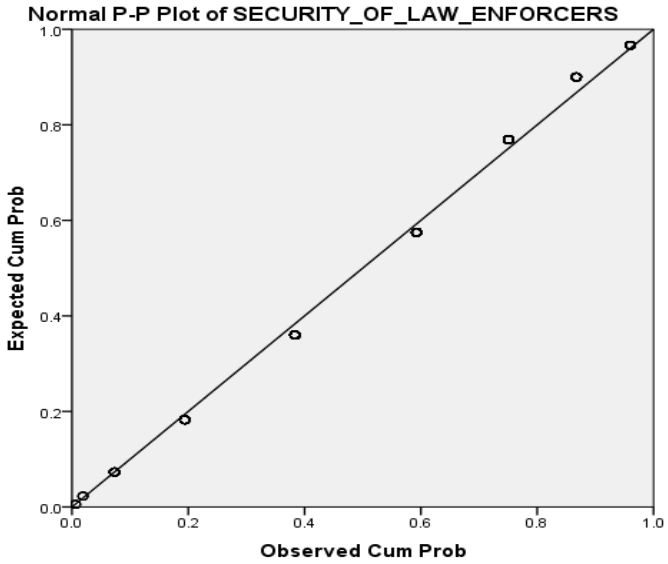

FIGURE 4. 3: SLE Normality Test

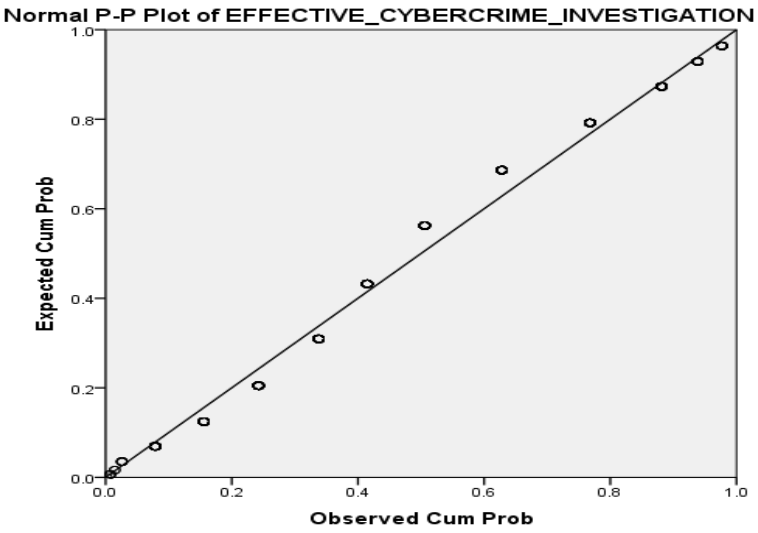

FIGURE 4. 4: ECI Normality Test

4.7.3 Multicollinearity Testing

The Variance Inflation Factor (VIF) was utilized in this study to detect multicollinearity.

TABLE 4. 19
VIF Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	.616	.149		4.137	.000	.323	.909		
	ITT	.213	.046	.230	4.663	.000	.123	.303	.527	1.896
	QQE	.560	.061	.513	9.176	.000	.440	.680	.411	2.434
	SLE	.080	.036	.096	2.246	.025	.010	.151	.699	1.430

a. Dependent Variable: EFFECTIVE_CYBERCRIME_INVESTIGATION

Based on the information presented in Table 4.19, the coefficient - collinearity output statistics reveal that the Variance Inflation Factor (VIF) values for the independent variables are below 10. This indicates that there is little to no multicollinearity among the independent variables.

4.7.4 Homoscedasticity Testing

Homoscedasticity is a statistical assumption stating that the residuals' variances remain constant regardless of the different levels of the independent variable. It posits that the dispersion or spread of the residuals remains consistent across all values of the independent variable(s). The graphical approach was employed in this study to assess homoscedasticity.

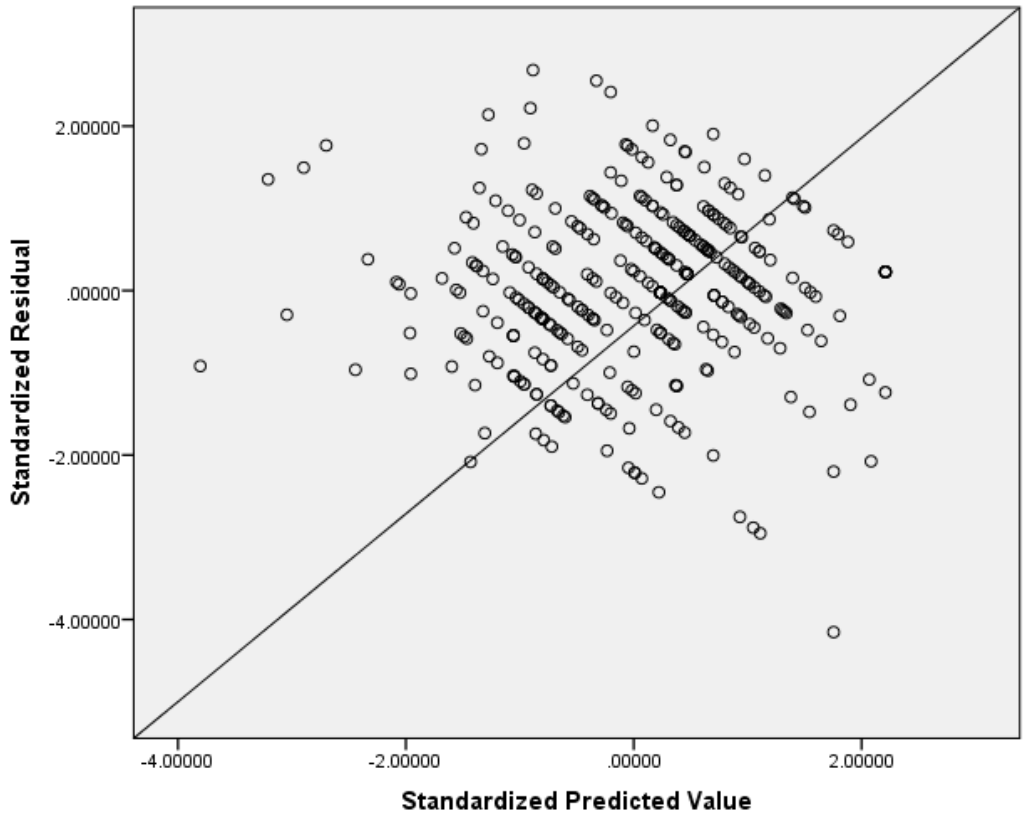

FIGURE 4. 5

Homoscedasticity Test

Based on the observations from figure 4.5, the scatterplot exhibits a random distribution, lacking a distinct funnel shape. This indicates that the spread of residuals remains relatively consistent across the entire range of predicted values. As a result, it is probable that the data fulfill the assumption of homoscedasticity.

4.7.5 Linearity Testing

The purpose of the linearity test is to determine whether there exists a linear relationship between the dependent variable and the independent variables.

TABLE 4. 20
Linearity Test ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
ECG * ITT	Between Groups	(Combined)	81.815	12	6.818	18.902	.000
		Linearity	75.784	1	75.784	210.109	.000
		Deviation from Linearity	6.031	11	.548	1.520	.122
	Within Groups		121.912	338	.361		
	Total		203.727	350			

According to the ANOVA table 4.20, the significance value (sig) for the deviation from linearity is 0.122, which is greater than the conventional significance level of 0.05. This result indicates that there exists a linear relationship between the independent variables, namely Information Technology Tools, Quality and Quantity of Evidence, and Security of law enforcers, and the Effectiveness of cybercrime investigation.

CHAPTER FIVE

DISCUSSION, CONCLUSION AND RECOMMENDATIONS

This chapter represents the final stage of the study, serving as a comprehensive summary of the research findings. It encompasses the conclusions drawn from the analysis and interpretation of the collected data. The primary focus is to address the research objectives and provide answers to the research questions initially posed at the beginning of the study. The conclusions highlight the key findings, their significance, and the relationships observed within the data, shedding valuable insights into the Regression Model of ICT Tools Usage in Cybercrime Investigation in Kenya. Moreover, this chapter also includes recommendations for future studies and limitations based on the research outcomes.

5.1 Findings Summary

The primary objective of this research was to create a regression model that could be applied in cybercrime investigations within the DCI (Directorate of Criminal Investigations) of Kenya. The study examined the relationship between three independent components, namely Information Technology tools, Quality and Quantity of Evidence, and Security of law enforcers, and their impact on the effectiveness of cybercrime investigation. Data for the study was gathered from police officers of different ranks within the DCI department. This study's demographic analysis, found that the DCI department predominantly male-dominated, with a significant portion of police officers belonging to the middle age group (31-40 years). The majority of them had 5-10 years of experience and held lower-level ranks, while their educational qualification was mostly at the secondary level. The descriptive analysis indicated that most respondents exhibited a level

of agreement with the variable statements. Among these variables, Quality and Quantity of Evidence received the highest level of agreement, with an average mean score of 3.70.

The correlation analysis revealed that the variables Information Technology tools, Quality and Quantity of Evidence, and Security of Law Enforcers exhibited positive relationships with the effectiveness of cybercrime investigation. Specifically, the Pearson correlation values were 0.610 for Information Technology tools, 0.723 for Quality and Quantity of Evidence, and 0.443 for Security of Law Enforcers. Furthermore, the ANOVA table provided strong evidence of the model's significance, with an extremely low sig-value of 0.000. This indicates a highly significant linear association among these three predictors and the effectiveness of cybercrime investigation.

The primary objective of the study was to utilize regression analysis to reveal key findings concerning the relationship between components of ICT tools and the effectiveness of cybercrime investigation. The results obtained from the regression analysis offered valuable insights into the significance and strength of these relationships. Among the variables under investigation, the most influential factor impacting the effectiveness of cybercrime investigation was found to be the Quality and Quantity of Evidence. A unit change in this factor resulted in a considerable positive change of 56% in the effectiveness of cybercrime investigation. Information Technology Tools also played a notable role, leading to a positive change of 21.3% in the effectiveness of cybercrime investigation. On the other hand, the impact of Security of law enforcers on the effectiveness of cybercrime investigation was relatively less significant, resulting in an 8% positive change.

Through the regression analysis, the study successfully identified the major drivers of effective cybercrime investigation among ICT tools components. Quality and Quantity of

Evidence emerged as the most crucial factor, followed by Information Technology Tools, while Security of law enforcers had a comparatively smaller impact.

5.1.1 Information Technology Tools and cybercrime investigation

The regression analysis carried out in this research revealed a notable impact of information technology tools on the effectiveness of cybercrime investigation. These tools encompassed aspects such as the implementation of automated programs and software, the usage of forensic tools, the utilization of global computer networks, and an increased focus on security vulnerabilities. The study revealed a statistically significant relationship between Information Technology Tools and cybercrime investigation. These findings align with Wekundah's (2023) study, which also suggested that the adoption of technology-based systems and models enhances the likelihood of effective cybercrime investigation. Similarly, Sigilai's (2021) study supported these results, emphasizing a positive correlation between information technology tools and the effectiveness of cybercrime investigation. According to the research, information technology tools have facilitated the extraction of valuable information from vast datasets, thereby bolstering the effectiveness of crime intelligence efforts.

5.1.2 Quality and Quantity of Evidence and cybercrime investigation

The regression analysis concerning the Quality and Quantity of Evidence exhibited a substantial impact on cybercrime investigation. This impact encompassed various aspects, including the vulnerability of internet service providers, the registration of domains and addresses, similarity in patterns of cybercrimes, the significant economic losses caused by cybercrimes, the continued rise in cybercrimes, and an increased number of cyber-attacks. Importantly, this construct was found to be statistically significant, reinforcing the validity of the findings.

These results are consistent with the conclusions drawn by Grigaliūnas and Toldinas (2020) in their study, which emphasized the efficacy of technology-based models in analyzing information derived from the forensic process, ultimately contributing to the overall effectiveness of cybercrime investigation. Likewise, a study conducted by Hasan et al. (2021) supports these findings by highlighting the value of artificial intelligence models in expediting cybercrime investigation through intelligence gathering.

5.1.3 Security of Law enforcers and cybercrime investigation

The conducted regression analysis in this research investigated the impact of law enforcers' security on cybercrime investigation. The security of law enforcers encompasses various aspects, including the number of arrests made in cybercrime cases, the utilization of forensic tools, and the efficiency of responding to reported crimes with the existing forensic resources. The study found a statistically significant relationship between law enforcers' security and cybercrime investigation.

These results are in line with the findings of a study conducted by Deflem and Shutt (2018), which also emphasized the importance of law enforcers' jurisdictional powers in ensuring information security. Their research highlighted the significance of effective coordination and cooperation among law enforcement agencies to effectively address cybercrime. The research establishes a clear connection between the security measures implemented by law enforcers and their impact on cybercrime investigation. The study's results, supported by previous research, underscore the crucial role that coordinated efforts among law enforcement agencies play in combating cybercrime effectively.

5.2 Conclusions of study

Information Technology Tools indicated that it had a positive relationship with effective cybercrime investigation. This was attributed to the significant impact these tools had on streamlining data analysis, facilitating digital evidence collection, and enabling faster information exchange among investigators. A comprehensive framework of cybercrime detection, incorporating advanced Information Technology Tools, could be beneficial for enhancing the overall effectiveness of cybercrime investigation.

Moreover, Quality and Quantity of evidence demonstrated a strong positive association with effective cybercrime investigation. This could be attributed to the fact that robust and abundant evidence provides investigators with the necessary information to build solid cases and identify culprits. High-quality evidence ensures accuracy and reliability in the investigative process, while an ample quantity of evidence increases the likelihood of identifying critical patterns and connections. This suggests that quality and quantity of evidence play a pivotal role in ensuring successful and effective cybercrime investigation.

On the other hand, the Security of law enforcers demonstrated a low positive association with effective cybercrime investigation. This could be attributed to certain limitations or constraints faced by law enforcement personnel, which might hinder their ability to fully leverage security measures in the context of cybercrime investigation.

Based on the findings of this study, it can be concluded that the usage of Information and Communication Technology (ICT) tools has a positive and significant influence on the effectiveness of cybercrime investigation within the Department of Criminal Investigations (DCI) in Nairobi. The research reveals that Quality and Quantity of Evidence demonstrated the strongest impact on the effectiveness of cybercrime investigation, followed by Information Technology

Tools. On the other hand, Security of law enforcers exhibited the least influence on the effectiveness of cybercrime investigation.

In conclusion, the contemporary digital ecosystem, marked by an overwhelming reliance on online platforms for commercial interactions, underscores the criticality of fortifying cybersecurity measures. The expansion of organized crime into the digital domain necessitates a comprehensive strategy, harmonizing technical solutions with legal interventions. As nations endeavor to bolster their resilience against cyber threats, the proactive involvement of both institutions and individuals emerges as a prerequisite to effectively mitigate risks and protect sensitive information.

5.3 Implications for DCI and policy makers

The findings of the study on the positive influence of ICT tools on the effectiveness of cybercrime investigation propose several recommendations to the Department of Criminal Investigations (DCI) in Kenya to enhance the effectiveness of cybercrime investigation. The DCI should prioritize the integration and adoption of modern ICT technologies in their investigative processes. This could include improving digital forensics capabilities, utilizing advanced data analytics tools, and enhancing cyber intelligence gathering methods.

In addition to that, Quality and Quantity of Evidence were identified as significant factors in determining the effectiveness of cybercrime investigation. Thus, it is crucial for the DCI to invest in training and resources to improve evidence collection techniques. This may involve providing specialized training to investigators on preserving and analyzing digital evidence.

Since Information Technology Tools were found to have a notable impact on the effectiveness of cybercrime investigation, it is important for the DCI to ensure its investigators are

well-versed in using relevant IT tools. Regular training sessions and workshops can help keep the investigators updated on the latest technologies and their applications in cybercrime investigation.

Although the Security of law enforcers had the least influence on the effectiveness of cybercrime investigation, it is still essential to prioritize the safety and security of investigators. Adequate training, equipment, and support should be provided to law enforcers to ensure they can conduct their work effectively and safely.

Besides technological advancements, raising awareness among the public about cybercrime and its implications would be essential. The DCI could initiate awareness campaigns and educational programs to help citizens protect themselves from cyber threats and report incidents promptly. Additionally, the DCI could consider collaborating with the private sector and academia to access the latest technologies and expertise in cybercrime investigation. Public-private partnerships and academic research collaborations can lead to more effective and innovative investigative practices.

The study indicates that Information and Communication Technology (ICT) tools have a significant positive influence on the effectiveness of cybercrime investigation. Policy makers could encourage and support the adoption of advanced ICT tools within law enforcement agencies. This could include providing funding and resources to equip investigators with the necessary technology and training to leverage these tools effectively.

In implementing these recommendations, the DCI and Kenya as a whole can strengthen their capabilities in cybercrime investigation, enhance public safety, and mitigate the impact of cyber threats on individuals, businesses, and the nation's security.

5.4 Recommendations for Further Studies

Nevertheless, it is crucial to acknowledge that the study's focus was exclusively on the Department of Criminal Investigations (DCI) within Nairobi. As a result, the general applicability of the findings to other DCI departments in different regions of the county might be restricted. To improve the external validity of the results and obtain a more comprehensive comprehension of the association between ICT tools usage and the effectiveness of cybercrime investigation, future research endeavors should consider expanding the scope to encompass a broader selection of DCI departments from various regions.

While this study focused on specific predictor variables, future research should also consider controlling for potential confounding variables that might influence the relationship between ICT tools usage and cybercrime investigation effectiveness.

Further research is needed to delve into the specific factors that contribute to the security of law enforcers' relatively lower impact and to identify potential areas for improvement in enhancing the role of law enforcer security in cybercrime investigation effectiveness.

Despite the significant correlation between the independent variables and effective cybercrime investigation found in the current study, as evidenced by a coefficient of determination of 61.6%, it is essential to acknowledge that 38.4% of the variance in effective cybercrime investigation remains unaccounted for within the confines of this research. Future researchers should conduct further investigations to explore additional factors that lie beyond the scope of this study, which might contribute to the unexplained variations in effective cybercrime investigation practices.

In pursuing these recommendations, future researchers can build upon the current findings, strengthen the understanding of the relationship between ICT tools and cybercrime investigation

effectiveness, and contribute to the development of evidence-based practices for combating cybercrime effectively.

REFERENCES

Asor, J. R. (2020). Implementation of Predictive Crime Analytics in Municipal Crime Management System in Calauan, Laguna, Philippines. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(1.3), 150–157.

Alberus, R. W. (2019). Translating a Digital Strategy for South Africa's Police Services. In *CONF-IRM* (p. 41).

Adesina, A. O., Ajagbe, S. A., Afolabi, O. S., Adeniji, O. D., & Ajimobi, O. I. (2022). Investigating Data Mining Trend in Cybercrime Among Youths. In *Pervasive Computing and Social Networking: Proceedings of ICPCSN 2022* (pp. 725-741). Singapore: Springer Nature Singapore.

Arroyo, J. C. T., Delima, A. J. P., & Orong, M. Y. (2020). Indexed Crime Data Visualization Utilizing Self-Organizing Map Algorithm. *International Journal of Emerging Trends in Engineering Research*, *8*(9), 5975–5978.

Akers, Ronald L., and Wesley G. Jennings. (2016). "Social Learning Theory." Pp. 230-240 in The Handbook of Criminological Theory, edited by Alex R. Piquero. Oxford: Wiley Blackwell.

Akers, Ronald L., Christine S. Sellers, and Wesley G. Jennings. (2016)(7th ed.). Criminological Theories. Introduction, Evaluation, and Applications. Oxford: Oxford University Press.

Asenahabi, B. M. (2019). Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches*, *6*(5), 76-89.

Bamanyisa, A. J. (2018). *The Effect of ICT Outsourcing on the Performance of Tanzania Police Force* (Doctoral dissertation, THE OPEN UNIVERSITY).

Bhardwaj, P. (2019). Types of sampling in research. *Journal of the Practice of Cardiovascular Sciences*, *5*(3), 157.

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa. In *ICIME 2011-Proceedings of*

the 2nd International Conference on Information Management and Evaluation: ICIME 2011 Ryerson University (p. 62).

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57, 24-41.

Chika,D.(2014).The Legal Framework and Institutional Arrangement on the use of ICT for Detection and Prevention of Criminality and Insecurity at All Levels in Africa. Tangier (Morocco)

Communications, A. (2021). Cybersecurity Sector Statistics Report Q1. https://www.ca.go.ke/wp-content/uploads/2021/12/Cybersecurity-Sector-Statistics-Report-Q1-2021-2022.pdf

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence.

Collier, B. (2020). Boredom, routine activities, and cybercrime during the pandemic. In *Cambridge Cybercrime Centre, COVID Briefing Paper 4*.

Cyoy, R. B. (2022). *Framework for Effective Management of Cyber Security on E-learning Platforms in Public Universities in Kenya* (Doctoral dissertation, university of nairobi).

Deflem, M., & Shutt, J. E. (2008). Law enforcement and computer security threats and measures. *Global perspectives in information security: legal, social, and international issues. New York: Wiley*.

Đalić, I., & Terzić, S. (2021). Violation of the assumption of homoscedasticity and detection of heteroscedasticity. Decision Making: Applications in Management and Engineering, 4(1), 1-18.

Farrow, K. (2017). http://www.crimes-ofpersuasion.com/Criminals/criminals.htm - accessed on 29.9.2017

Francis, B. G. (2016). *The use of ICT in criminal investigation processes in Tanzania: a case study of Dodoma region* (Doctoral dissertation, The University of Dodoma).

Garcia, N. (2018). *The use of criminal profiling in cybercrime investigations* (Doctoral dissertation, Utica College).

Guerra, C., & Ingram, J. R. (2022). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. Deviant Behavior, 43(1), 44-60.

Glen, S. (2022). "Cronbach's Alpha: Definition, Interpretation, SPSS" From StatisticsHowTo.com: Elementary Statistics for the rest of us! https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/cronbachs-alpha-spss/

Grigaliūnas, Š., & Toldinas, J. (2020). Habits attribution and digital evidence object models based tool for cybercrime investigation. *Baltic journal of modern computing*, *8*(2), 275-292.

Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*.

Hendricks, D.(2013). Technology Helps Continued Fight to Bring down American Crime Rates, www.huffingtonpost.com.

Hasan, R., Raghav, A., Mahmood, S., & Hasan, M. A. (2011, November). Artificial intelligence based model for incident response. In 2011International Conference on Information Management, Innovation Management, and Industrial Engineering (pp. 91-93)

Hewling, M.O. (2013), „Digital forensics: an integrated approach for the investigation of cyber/computer related crimes". PhD thesis. University of Bedfordshire.

Horan, C., & Saiedian, H. (2021). Cybercrime investigation: Landscape, challenges, and future research directions. *Journal of Cybersecurity and Privacy*, *1*(4), 580-596.

Jiang, B., Mak, C. N. S., Zhong, H., Larsen, L., & Webster, C. J. (2018). From broken windows to perceived routine activities: Examining impacts of environmental interventions on perceived safety of urban alleys. *Frontiers in psychology*, *9*, 2450.

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID-19 Pandemic. *International Journal of Information Engineering & Electronic Business, 13*(2).

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*(971), 971.

Kader, S., & Minnaar, A. (2015). Cybercrime investigations: Cyber-processes for detecting of cybercriminal activities, cyber-intelligence and evidence gathering. *Acta Criminologica: African Journal of Criminology & Victimology, 2015*(sed-5), 67-81.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81.

Lohr, S. L. (2021). Introduction. *Sampling*, 1–30. https://doi.org/10.1201/9780429298899-1

Luo, X. R., Li, H., Hu, Q., & Xu, H. (2020). Why Individual Employees Commit Malicious Computer Abuse: A Routine Activity Theory Perspective. *Journal of the Association for Information Systems, 21*, 1552–1593.

Leeney, D. (2018). *From Public Participation in Neighbourhood Policing to testing the limits of Social Media as a tool to increase the flow of Community Intelligence* (Doctoral dissertation, University of Cambridge).

Lalla, Himal & Flowerday, Stephen. (2010). „Towards a Standardized Digital Forensic Process: Email Forensics".

Li, Y., Li, J., Fan, Q., & Wang, Z. (2022). Cybercrime's tendencies of the teenagers in the COVID-19 era: assessing the influence of mobile games, social networks and religious attitudes. Kybernetes.

Lee, H. C., Palmbach, T. M., & Miller, M. T. (2001). Henry Lee's Crime Scene Handbook. San Diego: Academic Press.

Mbuba, J. M. (2021). Policing in the Republic of Kenya. *Global Perspectives in Policing and Law Enforcement*, 25.

Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*, *13*(11).

Moser, A., & Korstjens, I. (2018). Series: practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. European Journal of General Practice, 24(1), 9– 18.

Mmabatho, A. & Mofokeng, J. (2021). South African Police Service Capacity to respond to cybercrime: challenges and potentials. Journal of Southwest Jiaotong University, 56(4).

Mwakio, P., Mathenge, G., & Maroko, G. (2020). Assessing the Preparedness of Law Enforcement Agents in Dealing with White-Collar Crimes in Kenya: A Case of Nairobi City County. International Journal of Research and Innovation in Social Science, 4(7).

Mbaya, B. (2016). The State of Forensic Investigation in Kenya: Doctoral Dissertation, University of Nairobi. Kenya

Mohammed, H., Clarke, N., & Li, F. (2016). An automated approach for digital forensic analysis of heterogeneous big data.The Journal ofDigital Forensics, Security, and Law,11(2), 137.

Majid, U. (2018). Research fundamentals: Study design, population, and sample size. *Undergraduate research in natural and clinical science and technology journal*, *2*, 1-7.

Masombuka, M., Grobler, M., & Watson, B. (2018). Towards an artificial intelligence framework to actively defend cyberspace. In *European Conference on Cyber Warfare and Security* (pp. 589-XIII). Academic Conferences International Limited.

Magutu, P. O., Ondimu, G. M., & Ipu, C. J. (2011). Effects of cybercrime on state security: Types, impact and mitigations with the fiber optic deployment in Kenya. Journal of Information Assurance & Cybersecurity, 2011(1), 1-20.

Ngare, B. (2018) Factors contributing to cyber security framework in Kenya: a case study of Kenyan telecommunications companies

Ndikaru, W. T. (2021). Crime causes and victimization in Nairobi city slums. http://41.89.56.62:8080/handle/123456789/1790.

National Police Service Act (2011). https://nis.go.ke/downloads/National%20Police%20Service%20Act,%20No.%2011A%20of%202011.pdf

Opp, K. D. (2020). *Analytical criminology: Integrating explanations of crime and deviant behavior*. Routledge.

Onyango, D. A. (2022). *Determinants of Profitability on Street Vending in Kisumu Central Business District, Kenya* (Doctoral dissertation, University of Nairobi).

Opalo, K. O. (2018). Another disputed election batters Kenya's institutions. *Current History*, 117(799):187-193.

Odoyo, A. J., Abeka, S., & Liyala, S. (2020). Exploring a Social Learning Perspective on Computer Forensics Barriers and Factors Affecting Cybercrime Investigation in Kenya, 4(7).

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable children and youth studies*, *8*(4), 298-309.

Paat, Y. F., & Markham, C. (2020). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18–40.

Police Executive Research Forum. (2014). „The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime". Washington, D.C. 20036

Reith, M., Carr, C. & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, Vol. 1 No. 3.

Rupa, C., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A. (2020). Computational system to classify cyber crime offenses using machine learning. *Sustainability*, *12*(10), 4087.

Rossmo, D. K. (2021). Dissecting a criminal investigation. Journal of Police and Criminal Psychology, 36(4), 639-651.

Rossmo, K. (2022). The Anatomy of a Criminal Investigation. Criminologie, 1-26.
Serianu (2020), Kenya Cyber Security Report. Available at:

Sürücü, L., & MASLAKÇI, A. (2020). Validity and reliability in quantitative research. *Business & Management Studies: An International Journal*, *8*(3), 2694-2726.

Sager, M. A., & Afzal, A. (2022). Journal of ISOSS 2022 Vol. 8 (3), 296-312 IMPACTS OF POLICE INVESTIGATION ON LOW CONVICTION RATE & CRIMINAL JUSTICE SYSTEM: A STUDY OF DISTRICT FAISALABAD, PUNJAB, PAKISTAN. Journal of ISOSS, 8(3), 296-312.

Šarūnas, G., & Jevgenijus, T. (2020). Habits Attribution and Digital Evidence Object Models Based Tool for Cybercrime Investigation. Baltic J. Modern Computing, 8(2), 275-292.

Schoch, K. (2020). Case study research. *Research design and methods: An applied guide for the scholar-practitioner*, 245-258.

Shrestha, N. (2020). Detecting multicollinearity in regression analysis. American Journal of Applied Mathematics and Statistics, 8(2), 39-42.

Subair, S., Yosif, D. ., Ahmed, A. ., & Thron, C. . (2022). Cyber Crime Forensics . *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, *1*(1), 41–49. https://doi.org/10.54938/ijemdcsai.2022.01.1.37

Sileyew, K. J. (2019). *Research design and methodology* (pp. 1-12). Rijeka: IntechOpen.

Samoei, P. C. (2018). Role of Information Communication and Technology in Enhancing Security in Urban Areas in Kenya: A Literature Based Review. *Journal of Information and Technology*, *2*(1).

Suleiman, M. M., Kuliya, M., Surajo, A. Z., & Musa, J. (2020). Ict Is An Integral Strategy For Crimes Prevention And Detection. *Academic Leadership*, *21*(6), 249-257.

Sigilai, C. J. R. (2018). *Assessing The Impact Of Information Technology On The Gathering Of Crime Intelligence By DCI Investigators* (Doctoral dissertation, University of Nairobi).

Tanui, K. D., & Barmao, K. C. (2016). Use of ICT in the Detection and Prevention of Crime in Kenya. Journal of Information Engineering and Applications, 6(9).

Thakur, M. (2022, June 18). *Sample Size Formula*. WallStreetMojo.

Udanor, C. N., Ogbodo, I. A., Ezugwu, O. A., & Ugwuishiwu, C. H. (2020). A Logistic Predictive Model for Determining the Prevalent Mode of Financial Cybercrime in Sub-Saharan Africa. In *The International Conference on Emerging Applications and Technologies for Industry 4.0* (pp. 137-151). Springer, Cham.

Van, N. T. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. *International Journal of Cyber Criminology*, *14*(1), 156-173.

Valjarevic, A., & Venter, H. S. (2012, August). Harmonised digital forensic investigation process model. In *2012 Information Security for South Africa* (pp. 1-10). IEEE.

Wachs, S., Costello, M., Wright, M. F., Flora, K., Daskalou, V., Maziridou, E., ... & Hong, J. S. (2021). "DNT LET'EM H8 U!": Applying the routine activity framework to understand cyberhate victimization among adolescents across eight countries. Computers & Education, 160, 104026.

Walumoli, B. (2021). *A Critical Analysis of the Challenges Facing Countercybercrime in 21st Century Africa: a Focused Comparison of Kenya and Rwanda* (Doctoral dissertation, University of Nairobi).

Wu, Y., Xiang, D., Gao, J., & Wu, Y. (2019). Research on investigation and evidence collection of cybercrime cases. In *Journal of Physics: Conference Series* (Vol. 1176, No. 4, p. 042064). IOP Publishing.

Wekundah, R. N. (2015). *The effects of cyber-crime on e-commerce; a model for SMEs in Kenya* (Doctoral dissertation, University of Nairobi).

Wanderi, C. (2007). Computer forensics-Kenya needs a law to protect businesses against cyber/computer crime. Retrieved on 17th May 2015:

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119-1131.

Yusoff, M. S. B. (2019). ABC of Content Validation and Content Validity Index Calculation. *Education in Medicine Journal*, *11*(2), 49–54

Zhang, J., & Lei, Y. (2022). Trend and Identification Analysis of Anti-investigation Behavior in Crime by Machine Learning Fusion Algorithm. *Wireless Communications and Mobile Computing, 2022*.

Zaballos, A. and Herranz, F. (2013) From Cybersecurity to Cybercrime: A Framework for Analysis and Implementation. Inter America development crime.

APPENDIX I: QUESTIONNAIRE

My name is Brian, a Masters student in Faculty of Computing and Information Management. I am currently conducting a research entitled **"A REGRESSION MODEL OF ICT TOOLS USAGE IN CYBERCRIME INVESTIGATION IN KENYA"**. The Information collected will be treated as confidential and will be used for academic purposes of this study only. Thank you in advance for taking your precious time to fill this Questionnaire.

SECTION A

Demographic information of the respondents

1. What is your gender? Female □ Male □
2. Age group; 16-20years □ 21-30years □ 31-40years □ 41-50years □ over 51years □
3. Which Department do you work at of the Directorate of Criminal Investigations? Land Fraud Unit □ Anti-Banking Fraud □ Special Crime Prevention Unit □ Cyber Crime Unit □ Anti-Narcotics Unit □ Forensic Department □ Serious Crime Unit□ Ballistics Unit□
4. The number of years you have worked in the Directorate of Criminal Investigations? Less than 5□ 5-10□ 11-15□ 16-20□ over 20□
5. What is your rank? Top level□ Middle level□ Bottom level□
6. What is your highest level of education? No education □ Primary □ Secondary □ Certificate □ Diploma □ Degree □ Postgraduate degree □

SECTION B

7. Do you currently own any forensic tools used in cybercrime investigations? If Yes which ones?

.....

.....

.....

Kindly respond to the following statement in relation to your perspective on the extent to which information technology has enhanced security of police officers in the process of intelligence gathering. (Tick only one box for each item)

	To what extent has information technology improved on police investigation operations	**Very Great Extent**	**Great Extent**	**Moderate Extent**	**Small Extent**	**No Extent**
1	To what extent has automated software and programs enhanced investigations through intelligence gathering among police Officers?					
2	To what extent do you agree that there's internet connectivity in your offices within Nairobi County?					
3	To what extent do you agree that cybercrime is reported frequently?					

SECTION C

Kindly respond to the following statement in relation to your perspective on the extent to which information technology affect quality and quantity of evidence against cybercrime suspects. (Tick only one box for each item)

	Information technology and quality and quantity of evidence	**Very Great Extent**	**Great Extent**	**Moderate Extent**	**Small Extent**	**No Extent**
1	To what extent do you agree that there's increased number of cyber-attacks?					

2	To what extent is the similarity in pattern of cybercrimes?					
3	To what extent do you agree that vulnerable internet service providers can compromise evidence collection?					
4	To what extent do you agree that registering domains and addresses can secure intelligence sharing?					
5	To what extent do you agree that cybercrime impacts huge losses on the economy?					
6	To what extent do you think cybercrimes will continue to rise?					

SECTION D

8. How many arrests have been made in relation to cybercrime cases? Yes □ No □
   If Yes what's the average number of arrests since 2021?

.....

9. With the current forensic tools you own, what's the average response time of any reported cybercrime case?

.....

.....

SECTION E

Kindly respond to the following statement in relation to your perspective on the extent to which information technology leads to effective cybercrime investigation. (Tick only one box for each item)

No.	**Extent to which information technology leads to effective cybercrime investigation**	**Very Great Extent**	**Great Extent**	**Moderate Extent**	**Small Extent**	**No Extent**
1	To what extent do you agree that cybersecurity measures increases effective cybercrime investigation?					
2	To what extent do you agree that information technology tools increase the detection of cybercrime?					
3	To what extent do you agree that continuous training of staff on how to use the forensic tools increases effective cybercrime investigation?					
4	To what extent do you agree that there's continuous upgrade of cybersecurity tools within DCI?					

THANK YOU FOR YOUR COOPERATION