EFFECT OF DIGITAL FORENSIC ON CRIME DETECTION IN NIGERIA

BY

AJAYI, Oluwashina Joseph
NSU/IGDS/MSC/DGF/002/15/16

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, NASARAWA STATE UNIVERSITY, KEFFI, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE (M.Sc.) DEGREE IN FORENSIC INVESTIGATION (DIGITAL FORENSIC)

AUGUST, 2019.

DECLARATION

I hereby declare that this dissertation has been written by me and it is a report of my research work. It has not been presented in any previous application for a Master of Science (M. Sc.) degree in Forensic Investigation (Digital Forensic). All quotations are indicated and sources of information specifically acknowledged by means of references.

_____ _____

AJAYI, Oluwashina Joseph **Date**
NSU/IGDS/MSC/DGF/002/15/16

CERTIFICATION

This dissertation titled, "**Effect of Digital Forensic on Crime Detection in Nigeria**" meets the regulations governing the award of Master of Science (M.Sc.) degree in Forensic Investigation (Digital Forensic), School of Postgraduate Studies of Nasarawa State University, Keffi, and is approved for its contribution to knowledge.

Prof. S. A. S. Aruwa Chairman, Supervisory Committee	Date
Dr. Usman A. Yusuf Coordinator	Date
Dr. Abdul Adamu Internal Examiner	Date
Prof. Andrew E. Zamani Director, IGDS	Date
Prof. J. J. Adefila External Examiner	Date
Prof. J. M. Ayuba Dean, School of Postgraduate Studies	Date

DEDICATION

This work is dedicated to God Almighty.

ACKNOWLEDGEMENTS

My utmost appreciation goes to my supervisor Prof. S. A. S. Aruwa for your untiring effort towards making this work a reality. I also appreciate both the Director of Institute of Governance and Development Studies Prof. Olayemi Akniwumi and Dr, Abdul Adamu for their support. My appreciation also goes Mr Yahaya Abdullahi of the Institute and every other staff. I equally appreciate my Director Dr. Muhhamed Yau and my colleague, thank you so much. Also to my wife thank you for your enduring love and support throughout the period of putting this work together.

My unreserved gratitude goes to my parents; Mr and Mrs Enoch Adedeji Ajayi for their love since childhood, this has kept me going, and I thank you so much for it. Also to my siblings; Oluwaseun, Adedeji, and Folakmi, you are indeed the best, thank you all for being there for me.

I also appreciate all the defence panel members; Dr. Ismaila Olotu, Dr. Aza, Dr Hassan and others I could not mentioned, thanks for the constructive suggestions that has improved the quality of this work. To all those I could not mention, please accept my heartily gratitude. I appreciate every one of you.

TABLE OF CONTENTS

CHAPTER THREE

RESEARCH METHODOLOGY

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

LIST OF FIGURE(S)

Page

LIST OF TABLES

ABSTRACT

In the past years, digital forensics has become increasingly important in cases where electronic devices were used in the perpetration of a crime. This study examined the effect of Digital Forensics on crime detection in Nigeria. Specifically, the study centered on Computer forensic, Mobile forensic, and Network forensic as forms of Digital forensic and their effect on Crime detection were examined. The survey research design method was adopted for this study. The population of the study was 49 staff from three (3) law enforcement agencies. The instrument used to gather relevant data for the data was the questionnaire. Frequencies and percentages in cross-tabulations were used for describing the data. In testing the hypotheses for this study, Multiple Regression and ANOVA were adopted to examine the influence of the independent variables on the dependent variable. The findings showed that all forms of Digital forensic examined have significant effect on the detection of Crime. It was also noted from the result of the analysis that the rate of prosecution has increased since the adoption of digital forensic in Crime detection. It was established that relevant laws in Nigeria such as the Cyber Crime Act 2015, and Evidence Act 2011 enhanced the acceptance of digital evidence in a court of law. The study concluded that there is a significant effect of Computer forensic, Mobile forensic, and Network forensic on Crime detection in Nigeria. It was recommended that law enforcement agencies should continue to uphold the adoption of digital forensic in criminal investigation so as to further increase Crime detection in Nigeria.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

Over the past years digital forensics has become increasingly important in cases where electronic devices are used in the perpetration of a crime. The initial focus of digital forensic investigations was on crimes committed by using computers, but the field has expanded to include different devices where digitally stored information can be manipulated and used for various other criminal related activities.

A large amount of information is produced, accumulated, and distributed via electronic means. Recent study demonstrates that in 2008, 98% of all document created in organization were created electronically (Healy, 2008). According to Healy (2008) approximately 85% of 66 million U.S. dollars was lost by organizations due to digital related crime in 2007. Digital forensic investigations are common practice in law enforcement and commerce. Rapidly developing technology has resulted in various methods used by investigators to establish the root cause of an incident. This has in turn resulted in many digital forensic investigation approaches being proposed, developed and refined.

The need for the timely identification, analysis and interpretation of digital evidence is becoming more crucial with the spread of digital based evidence. According to a publication by National Institute of Justice (NJI), USA (2002), Computers are used for committing crime, and, thanks to the burgeoning science of digital evidence forensics, law enforcement now uses computers to fight crime. Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a Compact Disc (CD), and a flash card in a digital camera, among other places. Digital evidence is commonly associated with electronic crime,

or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. For example, suspects' e-mail or mobile phone files might contain critical evidence regarding their intent, their whereabouts at the time of a crime and their relationship with other suspects. To fight e-crime and to collect relevant digital evidence for all crimes, law enforcement agencies are incorporating the collection and analysis of digital evidence, also known as computer forensics, into their infrastructure.

In developing country like Nigeria, Digital Forensics is still at infancy and its being used to efficiently resolve cases that typically would not have been resolved. There are standard investigation procedures, tools and techniques that are accepted as standard of practice which is applicable to all various forms or types of Digital Forensics which will be studied as it applied to Digital Forensics in Nigeria. In many investigations, critical information is required while at the scene or within a short period of time - measured in hours as opposed to days. The traditional cyber forensics approach of seizing a system(s) or media, transporting it to the lab, making a forensic image(s), and then searching the entire system for potential evidence, is no longer appropriate in some circumstances. In cases such as child abductions, missing or exploited persons, time is of the essence. In these types of cases, investigators dealing with the suspect or crime scene need investigative leads quickly; often, it is the difference between life and death for the victim(s).

The usage of the Internet and Information Communication Technology has increased rapidly. Almost every valuable and confidential information is stored in computers or computer based systems and majority are sharing their personal information in social networks such as Facebook. There is a significant growth of the computer based or online criminals all over the

world due to the evolution of the information and communication technology. Criminals involved in murder, kidnapping, sexual assault, extortion, drug dealing, cybercrimes, economic espionage and cyber terrorism, weapon dealing, robbery, gambling, economic crimes, and criminal hacking e.g. Web defacements and theft of computer files, maintain files with convicting evidence on their computer.

In Nigeria, there are government bodies and agencies responsible for the investigation of Crimes which could either are Terrestrial or Cyber related. There is no better way to resolve Digital related crime other than engaging in the Digital Forensics process which have its own acceptable technique and processes which are generic to various types of Digital Forensics though approach may be different depending on the type or form of Digital Forensics engaged. The type engaged depend on the nature of the crime under investigation and the type of resources that are available. Often, the result of Digital Forensics Investigation results in court and all required fundamentals must be met. EFCC (Economic and Financial Crimes Commission) and ICPC (Independent Corrupt Practices and Other Related Offences Commission) are major players in detection and prevention of crimes alongside the NPF (Nigeria Police Force), the DSS (Department of State Services), and the NA (Nigeria Army) just to mention a few. Focus will be on EFCC, ICPC, and NPF in identifying the effect of using Computer Forensics, Mobile Forensics, and Network Forensics on Crime detection in Nigeria.

1.2 Statement of the Problem

Occurrence of crime is inevitable in our society. Once any of the following has occurred: a system or network has been compromised, a cybercrime has been committed, or there is a major financial fraud, it is essential to be able to sift through the evidence of what has

happened. Prior to the amendment of the Nigerian Evidence Act of 1990 in 2011, digital evidences are not accepted in court of law, it then means that any computer related evidences are null and void. The amendment has therefore accommodated evidences produced with a computer and those that affected the computers directly. Computer in the face of law according to section 258 of the Evidence Act 2011 as amended is any device for storing and processing information and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison, and any other process. This therefore includes Mobile phones, digital watches, cameras, Network systems e.t.c.

Furthermore, the Cyber Crime Act 2015 also supported digital evidences in cases where computer was used either as a tool or target of a crime. Crime has transcended borders with the aid of robust Information Technology platforms. Terrestrial crimes are no longer committed in isolation as every form of crime has a digital trace. For every crime that occurs, or is being planned, there are footprints always left behind by the perpetuator.

Adequate metrics are not available to help determine the success or failure of Digital Forensics techniques as applied by Law enforcement agencies in Nigeria. Equally, there are no clear-cut evidences to reflect whether the amendment of the Evidence Act in 2011 or the enactment of Cyber Crime Act 2015 has helped in the detection of crime.

This study therefore focuses on the effect of Digital Forensics used by EFCC (Economic and Financial Crime Commission), ICPC (Independent Corrupt Practices and Other Related Offences Commission), and Nigeria Police Force on crime detection.

1.3 Research Questions

The following questions guided this research and led ultimately to answer accurately the effect of Digital Forensics used in detection and prevention of crime in Nigeria. This research which is quantitative in nature answered the following questions;

1. How does Computer Forensics affect Crime detection in Nigeria?
2. What are the effect of Mobile Forensics on Crime detection in Nigeria?
3. In what ways does Network Forensics affect Crime detection in Nigeria?

1.4 Objectives of the Study

The main objective of this research was to study the effect of Digital Forensics on Crime detection in Nigeria. The specific objectives are to:

(i) examine the effect of Computer Forensics on Crime detection in Nigeria.

(ii) assess the effect of Mobile Forensics on the detection of crime in Nigeria.

(iii) examine the effect of Network Forensics on Crime detection in Nigeria.

1.5 Statement of Hypotheses

The study presented the following null hypotheses;

$H_{01:}$ Computer Forensics do not significantly affect Crime Detection in Nigeria.

H_{02}: Mobile Forensics do not significantly affect Crime Detection in Nigeria.

H_{03}: Network Forensics do not significantly affect Crime Detection in Nigeria.

1.6 Significance of the Study

Digital documents and storage devices hold the key to many criminal investigations in developed world. The purpose of engaging Digital Forensics is to use digital evidence as a means in prosecuting criminals and law offenders. Crime is gradually becoming an unfortunate artifact of today's wired and global society. It is no surprise that individuals involved in deviant and or criminal behaviour have embraced technology as a method for improving or extending their criminal tradecraft. With the proliferation of technology, our

notions of evidence and what constitutes potential sources of evidence are drastically changing. Gone are the days when evidence was mainly document based. This research identified three major types of forensics that can help in resolving crimes. The success recorded working with digital forensics was also accessed and recommendations were provided on identified areas of improvement.

This study is of importance to law enforcement professional by creating adequate awareness as to the effectiveness of Digital Forensics and its effect on Crime Detection as against the traditional method of investigation and as a result, they will align their investigations and enquiries to the techniques of used in Digital Forensic. I also believed that more researchers will investigate and improve on this new area of knowledge in Nigeria as this will further explore various aspect of Digital Forensic and consequently create an effective ways to detecting crime.

1.7 Scope of the Study

Section 84 of the Evidence Act, 2011 as amended strengthens the admissibility of statement in documents produced by a Computer; this makes Digital Evidence admissible in court. Also, section 258 defines Computer as any device for storing and processing information and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison, and any other process. Cyber Crime Act, 2015 equally supported evidences related to cybercrimes. These two (2) acts empowered the law enforcement agencies to present digital evidences in the prosecution of crimes. There are quite some numbers of agencies responsible for the investigation of crime in Nigeria. This study relied on the staff of Forensics Division of Economic and Financial Crimes Commission (EFCC), Independent Corrupt Practices and Other Related Offences Commission (ICPC), and Nigeria Police Force (NPF) as major sources in answering the

questions raised for this research using questionnaires which were administered within a month in 2018 and this project span through a period of 9 months.

CHAPTER TWO

LITERATURE REVIEW

2.1 Conceptual Framework

2.1.1 Concept of Digital Forensics

Peisert, Bishop, and Marzullo (2008) defined digital forensics as a branch of forensic science wherein investigation results are used to prove or refute accusations of crime committed by means of digital devices. Digital devices here include all electronic devices capable of storing and or processing data.

Palmer (2001) also defined Digital Forensic as the use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Another definition of Digital Forensics was given by Zatyko (2007) as the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation.

There are various forms of Forensics with equal responsibilities of providing evidence in resolving a crime. This include Computer Forensics which some use interchangeably as Digital Forensics but in the real sense, Digital forensics is all encompassing and it include other forms or types such as Mobile or Phone Forensics, Network Forensics, Live Forensics and so on. Computer, Mobile or Phone, and Network Forensics are discussed below.

2.1.1.1 Computer Forensics

Mohay, Anderson, Collie, McKemmish, and de Vel (2003) defined Computer forensics as the science of identifying, evaluating, and presenting digital evidence. There exists well-defined means and processes by which to accomplish the goals of this branch of science. Just as in other fields, one of the required and less glamorous steps in computer forensics is tediously documenting everything from whatever may have led to an investigation to how it has been conducted and what has been discovered. Selamat, Sahib, Hafeizah, Yusof, and Abdollah (2013) presented the framework for an investigation derived from the Digital Forensic Research Workshops (DFRWS) (2001) digital forensics process categories as follows: 1) identification, 2) preservation, 3) collection, 4) examination, 5) analysis, and 6) presentation. They defined the framework as varying by organizational policy and digital medium/device type.

Computer Forensics is of benefits to many organizations in various ways such as in the detection of Industrial espionage, Intellectual property theft, Professional spies and saboteurs, Dishonest or disgruntled employers, Spreading Malicious Programs and Inappropriate emails and internet use etc. Examination of Computer Forensics discloses content of email, metadata associated with files related to the crime with a possibility of revealing documents related to the crime as at the first time such document was created, the day it was last modified, when it was last saved or printed and which user has done these actions (Samanthi & Sunesh, 2016).

According to Samanthi and Sunesh (2016), there are many aspects of computer forensics investigation, at first investigators have ability to identify possible evidence to construct and proceed their investigation or search. Then they must select the most appropriate tool(s) for their investigation. The investigator must be aware with any number of methods and software

to avoid further damage while investigating. Because files may have been modified, damaged, deleted, corrupted or encrypted.

They further identified that Computer forensics involve with different types of evidence such as Inculpatory Evidence which supports a given theory, Exculpatory Evidence which contradicts a given theory and finally the evidence of Tampering which shows that the system was tampered with to avoid identification. Evidences will be accepted by courts based on the way of presenting, presenter's qualifications, reliability of the process used to preserve and analyse the evidence.

2.1.1.2 Mobile Forensics

Mobile phone proliferation is on the increase with the worldwide cellular subscriber base at 4 billion at the end of 2008 (Doran, 2008). While mobile phones outsell personal computers three to one, mobile phone forensics still lags computer forensics. Even when comparing sales figures of smart mobile phone devices which have some Personal Digital Assistant (PDA) capabilities, to the sale figures of the actual PDA devices, smart mobile phones sales continued to grow while the PDA figures continue to decline (Canalys, 2007). Data acquired from mobile phones continues to be used as evidence in criminal, civil and even high-profile cases (Aljazeera, 2005). Due to the exponential increase in the accessibility of individuals to mobile devices, most crimes committed, if not all has an element of digital connections and as such frameworks and techniques were put in place to acquire mobile phone data for crime prosecution.

Mobile phones applications are being developed in a rapid pace. Word processors, spreadsheets, and database-based applications have already been ported to mobile phone

devices (Westtek, 2008). The mobile phone's ability to store, view and print electronic documents transformed these devices into mobile offices. The ability to send and receive Short Message Service (SMS) messages also transformed mobiles into a message centre. Furthermore, technologies such as "push e-mail" and always-on connections added convenience and powerful communications capabilities to mobile devices. Push e-mail provided users with instant email notification and download capability, where when a new e-mail arrives; it is instantly and actively transferred by the mail server to the email client, in this case, the mobile phone. Among mobile Internet users, the most popular online activities are searching the Web, accessing news and sports information, downloading music, videos, and ringtones, using instant messaging, and using Internet email. Downloading music, videos, and ringtones has become the number one activity among mobile Internet users worldwide (Manfrediz, 2008). Most individual now uses their mobile phone or mobile devices are a major means of activities and hereby necessitate the need for Mobile forensics in resolving major crimes.

2.1.1.3 Network Forensics

Network forensics is an evolution of typical digital forensics, where evidence is gathered and analysed from network traffic. The concept of network forensics deals with the data found across a network connection mostly ingress and egress traffic from one host to another. Network forensics analyses the traffic data logged through firewalls or intrusion detection systems or at network devices like routers. The goal is to trace back to the source of the attack so that the cybercriminals are prosecuted.

Palmer(2001) defined Network forensics as the use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyse, and document digital evidence from

multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities.

Also, Ranum (2012) defined Network forensics as the capture, recording, and analysis of network events to discover the source of security attacks. Network forensics involves monitoring network traffic and determining if there is an anomaly in the traffic and ascertaining whether it indicates an attack. If it is so then the nature of the attack is also determined.

Network Traffic is captured, preserved, analysed and an incident response is invoked immediately. The large number of security incidents affecting many organizations and the increase in sophistication of these cyber-attacks are the main driving forces behind network forensics. The attacker is covering the tracks used to cause the attacks making it more difficult to trace back. Companies doing business on Internet cannot hide a security breach and are now expected to prove the state of their security as a compliance measure for regulatory purposes. Internet Service Providers (ISPs) are also being made responsible for what passes over their network (Perry, 2006). Hence, having the network forensics process in place will meet the requirements of the users, organizations, and ISPs. This in turn will support the prosecution of perpetrators.

Emmanuel, Joshi, and Rajdeep (2010) in their research proposed a framework as seen in figure 2.1 below. The proposed framework is generic as it aggregates many of the phases available in the digital forensic models but builds on those phases which are specific to

network forensics. They proposed a generic framework for network forensic analysis. They formalized a methodology specifically for network based digital investigation. The earlier digital forensic models focus on investigation of a standalone computer and interpretation of data stored in it. Computer forensics investigator has the advantage of specialized tools which the attacker lacked whereas the network investigator and the attacker are at the same skill level. The Difference is at the ethics level as the investigator uses the same tools and practices as the person being investigated (Berghel, 2003). Network forensics evolved as a response to the hacker community to discover and attribute the source of security attacks.

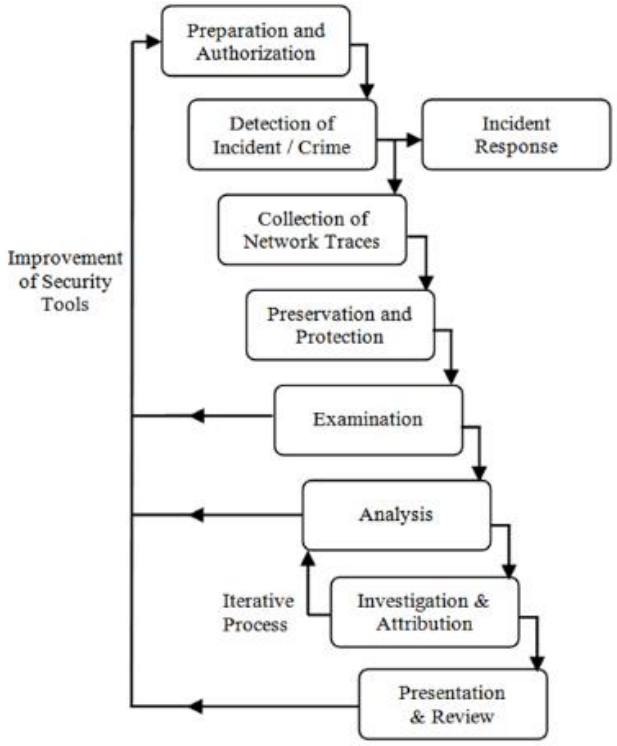

Figure 2.1: Framework for Network Forensics
Source: Emmanuel et al. (2010)

2.1.2 Concept of Crime Detection

Crime prevention incorporates not only the practices of the entire criminal justice system, but also those of many other social and public policies, as well as those of private citizens and private enterprise. Nigeria being a developing country is experiencing a rise in crime waves, criminal intentions and varying degree of delinquencies. The nature of these crimes includes

armed robbery, murder, rape, car theft, burglary, fraud, bribery and corruption, food and drug adulteration, gambling, smuggling, human trafficking, kidnapping, drug trafficking, money laundering, internet scam, advanced fee fraud and other illegal activities (Dambazau, 2007). There is no adequate will and genuine intention by any government to rid the society of the criminal tendencies and manifestations, as people in the leadership positions are also guilty of corruption and crime. An example of such flagrant disregard for diligent prosecution is the case of the former Governor of Delta State, Nigeria, Chief James Ibori who was found not guilty of corruption in Nigeria, but was prosecuted and found guilty of money laundering in the United Kingdom. The trial of many former Governors for corruption while in office has been going about 8 years with no end in sight, while they have moved on to other political offices while the trial drags on without diligent prosecution.

Dambazzau (2007) defined crime as a pattern of attitudes and behaviours directed both at reducing the threat of crime and enhancing the sense of safety and security to positively influence the quality of life, and to develop environments where crime cannot flourish. It is also the anticipation, recognition and appraisal of crime risk and the initiation of some action to reduce or remove it. He further asserts that crime control involves the idea of solving crime problems, arresting suspects, prosecuting and incapacitating offenders. The control of crime, therefore, deals with the immediate situation and rests on the discovery of past criminal behaviour.

The establishment of other agencies like State Security Service (SSS), Independent Corrupt Practices and other offences Commission (ICPC), and the Economic and Financial Crimes Commission (EFCC) is a laudable effort towards crime prevention and control, their narrow focus and few personnel inhibits them from functioning in a broad day to day manner like the

police. Some of them apart from the State Security Service that is consigned to the gathering of intelligence reports do not exist even at the State or Local Government levels. This leaves the day to day policing of the entire country more at the door-steps of the police. The capacity of the police and other security agencies in Nigeria to effectively prevent, detect and control crime has often been called to question. As a matter of fact, many have lost faith in the security agencies going by the incessant increase in the crime rate.

According to Okunola (2002), crime prevention basically involves the disruption of mechanisms, which cause crime events. In other words, the central question to crime prevention is how to disrupt the causes of crime. Crime prevention is a pattern of attitudes and behaviours directed at both reducing the threat of crime and enhancing the sense of safety and security to positively influence the quality of life and to develop environments where crime cannot flourish. Also, crime prevention is defined as "the anticipation, recognition and appraisal of a crime risk and the initiation of some action to remove or reduce it. Crime prevention involves the community, government as well as individuals; crime control involves the whole of the criminal justice system, that is, the police, courts and prisons while crime detection is the responsibility of security agencies. Here, several techniques and tools are engaged to aid prompt resolution of crime and hence serves as a deterrence to committing crime.

2.2 Empirical Review

2.2.1 Computer Forensics and Crime Detection

Computer Forensic investigation is usually associated with the investigation of computer-related crimes, which may include corruption, fraud, embezzlement and other white-collar crimes (Van Rooyen, 2004). According to Van der Westhuizen (1996), the systematic search

for the truth with the primary purpose of finding a positive solution to a crime with the help of objective or subjective clues forms the basis for Investigation. Investigation occur mostly to detect an already committed crime, however, more can also be done in preventing its occurrence. It is noted that the advancement in technology has seen criminals exploits various opportunity for illegal activities.

A challenge for the investigation of these illegal activities is that law enforcement officials hardly recognise the potential for technological evidence to help solve crimes and prosecute criminals. It appears that the ethos of law enforcement is inclined to be more attentive on the collection and inspection of non-technological evidence (Galves & Galves, 2004). According to Craiger and Shenoi (2007), the motive behind investigators focusing on traditional physical and/or document-based evidence is because of lack of knowledge and often due to lack of resources to deal with evidences gathered from this crime.

Galves and Galves (2004) also pointed out that criminals integrate technology into their range of activities but that in the respective roles of upholding justice, investigators, prosecutors, and even judges do not always develop adequate knowledge of technology, especially with respect to courtroom evidence. Because of inadequate education, training and awareness, law enforcement agents are unwilling to compromise cases by attempting processes, and the judiciary unwilling to try out procedures, with which they are unfamiliar, as emphasized by Craiger and Shenoi (2007).

Galves and Galves (2004) make known that digital technology has enabled the commission of crimes by criminals who previously may have found that committing crimes the old-fashioned way, such as by robbing, involved a great deal of risk or effort. Chisum and Turvey (2000) indicate that the Locard principle states that if two objects touch each other every contact leaves a trail. This means that incriminating information, which includes potential

electronic evidence, is always left behind by even the most advanced criminals, including everyone using computer and electronic device for any kind of activity. This electronic or audit trail, as mentioned by Galves and Galves (2004), can be used to present significant legal of evidence against an assumed criminal. According to these authors, this is because the electronic trail exposes an outstandingly probative "digital fingerprint" that can potentially be used to prove a criminal conduct in a court of law.

Technically, crime investigations suggest that few investigators are well-versed in the evidentiary, technical, and legal issues related to forensic electronic evidence, such as uncovering evidence without conceding its integrity or credibility and the standard or requirements for admitting electronic evidence at a trial. Consequently, most investigators at our various law enforcement agencies are not trained in computer crime investigations. Casey (2004) points out that electronic evidence is often overlooked, or collected incorrectly, and analysed ineffectively. This therefore suggests that there is a possibility that valued evidence is ignored by law enforcement, which may result in dropped or reduced charges as well as wrongful convictions (Craiger and Shenoi, 2007).

Computer Forensic is a tool that can help in the detection and prevention of various crimes. Acccording to Vacca (2005), great research emphasis should be placed on the computer forensic field of study, coupled with adequate training of the professionals involved in this field. Adequate training will ensure that the right skills are put in place as needed to detect and prevent criminal activities. Procedures and best practices to uncover electronic evidence without compromising its evidential value at trial are of importance to the field of Computer Forensics. The most important aspect of Computer Forensic is to find or explore evidence which is defined as the means of proving or disproving facts in dispute. It covers all the information and material submitted to a court by the parties concerned to enable the ruling officer to judge and settle a dispute (Joubert, 2001).

Van Rooyen (2004) suggested that investigators must always execute their mandate within the ambit of the law and its limitations. Swanson, Chamelin and Territo (2003) also pointed out that in investigating, while analysing, the investigators should strive to search for the truth. Joubert (2001) maintained that evidence must be collected in accordance with the constitution and relevant laws, example of such law is the Evidence Act 2011 as amended. Considering the above, and as indicated by Shah (2002), the investigator should always recognise the law and human rights.

Fisher (2004) and Lambrecht (2001) pointed out that a proper investigation that can lead to presentation of evidence in a court of law can only be ensured through a combination of scientific and investigative methods and techniques. Holmes (2006) explores the history of detectives, explaining that the first police detectives were established in England during the seventeenth century and that this was followed by France in the eighteenth century. Palmiotto (1998), in tracing how detectives were established in France, suggests that the detectives were founded by a former convict who believed that it takes one criminal to catch another. This means to say that every forensic investigator needs adequate knowledge about how crimes are or could be committed.

The evolution of Computer forensic investigators can be attributed to the growth in criminal activities that extended beyond country borders, which as a result necessitated cooperation by states to address international criminal activity. This situation, as shown by studies like O'Hara (1962), led to the establishment of the International Criminal Police Commission in the nineteenth century, today known as INTERPOL. The concept of specialised criminal investigation, as indicated by Ward (1975), started developing during this period. Karagiozis and Sgaglio (2005) suggested that forensic investigation has even earlier roots, starting in ancient Greece when the king suspected the royal jeweller of defrauding him in the making of his crown.

Corporate, private security and public sectors also have a legal responsibility to conduct criminal investigations with in this case might not necessarily end up in court of law. This supports the view of Rooyen (2004) when mentioning that corporate bodies, government departments and the private investigation industry have created their own internal investigation structures which are built on adequate internal control. An explanation of this is that various statutes also confer a certain degree of investigative powers on corporate bodies and government departments, as noted by Swanepoel (2001).

According to Shah (2002), the police have been given certain legal powers to enable them to perform their task of finding out clues to offences and working out these clues to fix the problem. This, however, does not imply that only the police have exclusive rights to investigate, as noted by Swanepoel (2001). The collected evidence is then referred to the prosecuting authority as it is believed by Marud (2004) that all role players should share information in their efforts to combat crime.

The basis of Computer Forensic Investigation is the ability of the crime scene investigator to be able to recognise the potential and importance of evidence at crime scene (Lee, Palmbach and Miller, 2003). This is an indication that intuition and an eye for what needs to be done as also suggested by Fisher and Fisher (2003) are some of the qualities required from an investigator. Some of the qualities of an investigator are brought to light in the study by Swanson *et al.* (2003), as follows, being able to not act out of malice or bias, discipline, use of own initiative and resourcefulness, being ethical and always using legally approved methods and ability to influence and win the confidence of the people they interact with. This supports the view of Vadackumchery (2003) that sincerity, honesty and integrity are vital qualities of an investigator which will assist in crime detection.

According to Simms and Petersen (1991), a Computer Forensic investigator is responsible for Identifying the occurrence of offenses, compiling reports on the circumstances surrounding the occurrence, interviewing victims, witnesses and suspects with the objective of identifying the offender and gathering sufficient evidence to allow prosecution to proceed. The responsibilities of an investigator are summarised by Horswell (2004) are as follows, assessment of the crime scene, control of the crime scene, examination of the crime scene, interpretation of the evidence, recording of the crime scene, evidence collection and case management.

For crime to be detected or prevented, necessary questions such as the 'Who?', 'What?', 'Where?', 'When?', 'Why?', and 'How?' are importance in conducting proper investigation (Van Rooyen, 2004). The objective of investigation is to determine if certainly an offence has been committed, then identify and apprehend the suspect, recover the stolen property and assist in the prosecution of the person charged with the crime (Bennett & Hess, 2004). Fisher (2004) and Golden, Skalak and Clayton (2006) agree with this view and add that the objective of investigation is to prove an unlawful action. According to Marais and Van Rooyen (1994) the objectives of an investigation is situation identification which involves making an observation at a crime scene to identify the crime committed, which is followed by gathering evidence. According to Weston, Lushbaugh and Wells (2000), the objective of crime investigation is to determine the truth, as far as it can be discovered in any Computer Crime inquiry. This inquiry by the Computer Forensic investigator will dwell on evidence acquired during the investigation.

Keane (2000) indicates that evidence is information which tends to prove facts in a court of law. Rooyen (2004) further explains that evidence may be presented either orally or physically by means of documents that are admissible to assist the court to reach a conclusion. Accordingly, the concept 'electronic evidence' in the context of the above-

mentioned definition of evidence is described by Volonino (2003) as referring to information that is stored electronically on a computer and that can be used as evidence at trial.

Kovacich and Boni (2000) point out that nowadays people are increasingly computer literate and use computers in every aspect of their lives. According to Lange and Nimsger (2004), the advancement of computers has therefore created an entirely new source of evidence in investigations referred to as 'electronic evidence'. Electronic evidence is defined by Casey (2000) as any electronic information created on a computer that can link a crime and a suspect. It should however be noted that other possible locations where electronic evidence can reside in the graphic provided by Lange and Nimsger (2009) also includes but not limited to; optical disks, floppy disks, remote internet storage, handheld devices, memory cards, servers and emails. This kind of evidence as indicated by Silvernail (1997) may be created at any stage once a person starts to use and enter information into a computer.

Computer Forensic aid in the revealing and recovery of embedded information which creates a link between the creator and the user of information as discussed by Taylor (2003). Gallagher and Aro (2005) emphasise that the embedded codes remain stored on a computer and can track usage and transmission of information back to the originator of the electronic information. On the other hand, as mentioned by Raysman and Brown (1984), a printed document may not show its history, for instance: the origins, contacts or edits carried out in the document. According to Raysman and Brown (1984), one can surely get background information about the origins of electronic evidence. Shira, Scheindlin and Rabkin (2000) validate this view by mentioning that electronic information potentially contains a wealth of hidden information that simply does not exist in a paper document. A deduction can be made from the above information that it is not easy to destroy electronic evidence, and this is of great benefit to an investigation.

According to Robbins (1999), electronic information generally is very mutable and easily altered with a few simple keystrokes; however, it is not easy to remove or delete an electronic document totally. Lange and Nimsger (2004) explain that a trace of electronic evidence tends to remain on the computer's hard drive even after deletion of the information which is a sort of good news to Computer Forensic investigator. As mentioned by Kozushko (2003), copies can remain in hidden places when criminals attempt to destroy electronic evidence.

Stippich (2006) confirms that electronic information is easy to manage compared to paper documents, which are labour intensive to manage. Hrycko (2007) also mentions that for paper documents more time and quite complex methods may be required to search for a information, while standard office computers could search all of the documents for precise information in far less time. This is because electronic versions of documents are used as evidence to substantiate computer fraud.

Cross (2008) indicates that the investigation and collection of electronic evidence from the computer remain the primary responsibility of law enforcement. Cardwell, Clinton, Cohen, Collins, Cornell, Cross, Depew, Ehuan, Gregg, Jean, O'Shea, Reis, Reyes, Scheler, Schneider, Schroader, Varsalone, Wiles, and Wright (2007) explain that investigators obtain such electronic evidence in order to link a suspect to a crime. According to Bryant (2008), the collected electronic evidence is used in investigations to support an enquiry and a subsequent prosecution. It is therefore of great importance, as mentioned by Stephenson (2000), that the evidence be collected properly and legally because if it is not it will be excluded as evidence in court. This then, as suggested by Bryant (2008), calls for an investigator with specialist knowledge in handling electronic evidence to use well-established investigative techniques to collect such evidence.

According to Vacca (2005), the established general forensic procedures to be followed in investigating electronic evidence include but are not limited to identification, preservation, acquisition, authentication and analysis. It is observed that the collection of electronic evidence is one of the phases in the investigation process and is often referred to as the acquisition stage. It is therefore also important to elaborate on the other phases of the general forensic processes relating to the investigation and to discuss the collection of electronic evidence as part of this process.

These international standards relating to the collection, analysis and presentation of electronic evidence as referred to by the expert participants were, according to Mohay, Anderson, Collie, De Vel and McKemmish (2003), drafted in 1997 by the Association of Chief Police Offices (ACPO) of England, Wales and Northern Ireland and were entitled Best Practices Guide for Computer Based Evidence. In 1998, as mentioned by these authors, the United States (US) established a working group that was assigned to craft cross-disciplinary guidelines and standards for the collection, analysis, preservation, and presentation of electronic evidence.

According to Mohay *et al.* (2003), the United Kingdom good practice guide and the SWGDE draft standards were reviewed in meetings and a workshop held by the IOCE during the International Hi-Tech Crime and Forensics Conference (IHCFC) in October 1999. A set of principles were presented and approved at that conference. These principles were also formalised in 2001 at the 13th International Criminal Police Organization (INTERPOL) Forensic Science Symposium and are outlined by Pollitt (2001) as follows: upon seizing digital evidence, actions taken should not change that evidence, when it is necessary for a person to access original digital evidence, that person should be competent, all activities relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review, an individual is responsible for all actions

taken with respect to digital evidence whilst the digital evidence is in their possession and any agency which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

The objectives of crime detection and investigation include the following; identification of crime, collection of evidence, identification of the suspect, securing the attendance of the accused in court, recovery of stolen property and prosecution are discussed in the sections below.

2.2.2 Mobile Forensics and Crime Detection

Modern communication technology has made the world a global village (Martins, 2009). Mobile phone is one of the devices that have revolutionized the mode of communication in the world today. Other devices include; computers, tablets, iPads, iPhone and fax. The diffusion of mobile phones in the rural areas of the developing world appears to be the next frontier (Kalba, 2007). This study will focus on mobile phone forensic evidence. Today there are over 7.22 billion mobile phones in the world. In the normal course of life or business most people are likely to use their mobile phones for taking pictures, sending or receiving text messages, accessing the internet to send or receive e-mail, record a video, play music, and or send or receive instant message service (Amanda, 2010). These phones keep records which can be extracted through mobile forensic investigation (Det, 2011).

Photographs, video and audio recordings taken by eyewitness at the scene using their mobile phones can or may be accepted as evidence in a court of law. According to Omeleze and Venter (2015), there are models for acquiring digital evidence using mobile phone. They also found out that many criminal activities have gone unsolved due to lack of sufficient evidence to convict the perpetrator. However, they argue with the evolution of mobile technology, with advanced features such as photo, video and voice recording options can transform such

devices into real-time potential digital forensic evidence-capturing devices (Omeleze & Venter, 2015).

The Mobile forensic investigator should have the potential acquired through training to capture potential digital evidence from mobile phones and preserve the integrity of such evidence taking into consideration the privacy policies, laws and ethics that may apply to the digital evidence presentation in criminal or civil proceeding (Omeleze & Venter, 2015). This will require using the right tool which are expensive and easily not affordable. It is important to use appropriate and licensed tools to maintain the forensic integrity of the acquired data (Omeleze & Venter, 2015).

O'Shea and Darnell (2011) discussed the admissibility of Forensic Mobile Phone Evidence. Basically, the article covers mobile phone forensics, technical and evidentiary issues. Paul (2005) on the forensic analysis of mobile phones assess the forensic soundness of the underlying methods used to acquire the data and the legal admissibility of information acquired by such methods as evidence in a Court of law. Sean (2008) discusses an overview of the forensic significance and legal implications of mobile phones.

Andrew (2009) documents in detail the methodology used to examine mobile electronic devices for data. His methodology encompassed the tools, techniques and procedures needed to gather data from a variety of common device. Rick, Sam, and Wayne (2013) discuss procedures for the data acquisition, examination and analysis, preservation, and presentation of digital evidence. They address the issue of ever increasing backlogs for most digital forensics labs and guidance on handling on site triage casework. The objective of the guide is twofold; to help organizations evolve appropriate policies and procedures for dealing with

mobile phones and to prepare forensic specialists to conduct forensically sound examinations involving mobile phones.

Generally mobile forensic investigations encompass seizure, acquisition and analysis of data recovered from a mobile phone (Sam, 2009). The examiner must always develop a report documenting any pertinent information while preserving integrity of the acquired data (Andrew, 2009). As earlier mentioned, some of the types of data that may be contained and saved in a mobile phone include call times, dialled and received calls, text messages, contacts, address book entries, residential addresses and email addresses, calendar items, photos, graphics and videos. Such information stored on and associated with mobile phones can be forensically obtained and can help address the crucial questions in an investigation, revealing whom an individual has been in contact with, what they have been communicating about, where they have been and what they have been doing (Gary, 2001).

For example, in the United States of America the Tampa Bay Time's Newspaper reported how Ronald Williams somehow activated his mobile phone which then called his wife's mobile phone while he was killing her. The voice mail recorded the killing with Williams threatening to kill his wife, and Mariama Williams screaming in terror during the attack in their St. Petersburg home. During the trial, the assistant state attorney Walter Manning produced a four-minute fatal stabbing recording. This was key piece of evidence in Ronald Williams's first-degree murder trial. He was convicted of first-degree murder and sentenced to death (Curtis, 2011).

Similarly, the United Kingdom (UK) media in an Investigation into the death of 15-month-old, Charlie Hunt showed how Darren Newton filmed himself on his mobile phone repeatedly

assaulting and doing other acts of cruelty to the 15-month-old Charlie Hunt. Newton recorded footage of Charlie as he sat shivering in a bath after the water had been let out and later that same day filmed himself hitting Charlie on the head repeatedly, giving the clip the title Happy Slap. The video clips were found on the mobile phone after Charlie died in hospital from serious head injuries and used as evidence against him. Relying on this mobile phone information, the Court convicted Newton and sentenced him to 24 years behind bars (Jaya, 2010).

According to Curran, Robinson, Peacocke, and Cassidy (2010), methods for acquiring data from mobile phones mainly depend on the condition, model, time and nature of the case. The current methods used all over the world are; manual acquisition, logical, file system and physical acquisition (Keonwoo, 2007). The forensic examiner manually scrolls down through the phone folders using the keypad and display of mobile phone when the phone is on (Sam, 2009). This is the first method commonly applied by examiners in Kenya. The examiners document each item. For example, the examiner may scroll up and down the contacts folders, messages, browser, settings, backup, calendar, clock, google, photos, videos, notebook, music, games, sim tool kit, facebook, whatsapp, play store, camera, to do list, calculator, FM radio and many other folders that a phone may contain depending on the model, design and make of the phone (Sam, 2009). This suggests only data accessible through the operating system is retrievable. Hidden and deleted data cannot be retrieved using manual acquisition. However, it is fast, works on almost every phone, requires no cables and is easy to use (Brain, 2002).

Logical acquisition involves a bit-for-bit copy of a mobile phone entire storage (Keonwoo *et al*, 2007). For instance, one can copy the contacts, messages, browser information, calendar

information, gallery, video, notebook, music, and downloads file. Copy of image is done to guarantee the integrity of data during analysis process. The benefits are it acquires information from the mobile phone using original applications in the phone, produces the specific file requested, and extracts data that is accessible through the operating system (Keonwoo *et al*, 2007). On the one hand, file system acquisition is useful in the understanding of the file structure, and provides access to deleted data from mobile's internal memory and also extracts hidden data from the phone (Satish, Rohit & Heather, 2016).

On the other hand, physical extraction recovers deleted data (including system and network provider information like previous International Mobile Subscriber Identity (IMSI), translate coded data, can retrieve data from devices where no SIM is present, bypass (and retrieve) handset security codes and acquire information from password-protected mobile applications such as Facebook, Skype, Whatsapp and browser-saved passwords (Richards, 2012). It can also create a comprehensive memory image and is also useful for memory card analysis. It provides scientifically reputable repeatable reliable evidence through the analysis of physical evidence acquired (Satish *et al.* 2016). It is important to know that when data is acquired from a mobile phone it is scrutinized to confirm any connection to the issue under interrogation. The examination and analysis depends on the type of evidence required to prove the existence of the fact in question.

The choice of tools used to extract data from a mobile phone mainly depends on the design and type of mobile phone in examination (Det, 2014). 'Universal Forensic Extraction Device' (UFED) is the mostly commonly used mobile phone forensic hardware tool; it is a product from Cellebrite (Whitfield, 2012). It is a hand-held device with optional desktop software, data cables, adapters and other peripheral. It does not require any computer software to

perform its tasks, it is packaged with report management and analysis software (Hoog, 2014). It can be used for in-field data extraction and analysis under adverse conditions (Osborne, 2012). It also can extract both physical and logical data from mobile phones such as cellular phones and other hand-held mobile phones, including the ability to recover deleted data and translate coded and password protected information. This implies that whatever activities, sites visited, messages sent or received, call, video, photographs and downloaded applications saved or deleted either in known languages or not direct words can be retrieved whether there be a password or not (Det, 2014).

Some of the challenges experienced extracting data include, ignorance, volatile data (Satish *et al*, 2016), rapid change in technology (Katie & Eric, 2016), Jurisdiction (Nelly, 2016). Some of the mobile crimes are global in nature. The constant change of technology has produced different models and design of mobile phone in the market with different brand-name and operating systems (Det, 2014). These mobile phones keep daily record of the calls made, text messages sent or received, internet sites visited, videos and photographs. This data is accessed through mobile forensic investigation and are used in the conviction of crime.

2.2.3 Network Forensics and Crime Detection

Modern communications networks can be used by the unscrupulous for purposes ranging from cyber-attack, terrorism and espionage to fraud, kidnap and child sexual exploitation. A successful response to these threats depends on entrusting public bodies with the powers they need to identify and follow suspects in a borderless online world (Anderson, 2015). As society evolves and technology marches forward our understanding of the origins of criminality must be continuously revised. The persistence, prevalence and seriousness of cyber-crime offending demands a greater response from the international

community. Technology is now deeply enmeshed within the fabric of society. Criminals understand that technology is a highly effective force multiplier which can be abused to enable illicit activity, and leveraged to facilitate access to a global constituency of victims living online. Our collective dependency on technology makes this threat extremely difficult to eliminate. The relative ease with which offenders engage in cyber-crime, and the high gains afforded to perpetrators, ensures that motivation for reprobates and recidivists remains strong.

Manifestations of crime emanating from the cyber domain are among the most formidable challenges for workers in criminal justice systems worldwide. The magnitude of this challenge is clearly acknowledged by the US Intelligence Community who classify 'cyber' as the prime global threat to national security, ahead of 'terrorism', 'proliferation of weapons of mass destruction', and 'transnational organized crime' (Clapper, 2015). Network Forensics Investigation is now expected to create proactive measures to counter a growing threat which is highly organized, well-funded, and immensely lucrative.

Following the escalations in reports of serious cyber-crime, one would expect to see a corresponding increase in conviction rates (Broadhurst, Grabosky, Alazab, Chon, 2014; Kaspersky Lab, 2015; Ponemon Institute, 2015). However, this has not been the case with many investigations and prosecutions failing to get off the ground (Zavrsnik, 2010; Frolova, 2011; Onyshikiv & Bondarev, 2012). The chief causes of this outcome may be attributed to trans-jurisdictional barriers, subterfuge, and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime. In the same way that science influences the utility of forensic inquiry, the capacity of investigators, prosecutors, judges and jurors to understand illicit use of technology also directly impacts conviction rates (Dubord, 2008; Leibolt, 2010). The ease with which cyber-crime crosses national borders, irreconcilable differences between national legal

frameworks, and deceptions employed by cyber criminals impedes attribution, and prevents crime fighters from interrogating suspects and apprehending offenders.

Cyber-crime offending can be technically complex and legally intricate. Rapid advancements in the functionality of information communication technologies (ICTs) and innate disparities between systems of law globally are stark challenges for first responders, investigating authorities, forensic interrogators, prosecuting agencies, and administrators of criminal justice. It is critically important to explore factors impeding investigation and prosecution of cyber-crime offending to raise awareness and expose these barriers to justice.

Cyber-crime is one of the major crime investigations by Network Forensic Experts. Technical experts, police, lawyers, criminologists, and national security experts understand the concept of 'cyber-crime' differently (Alkaabi, Mohay, McCullagh & Chantler, 2010). It is increasingly unclear whether cyber-crime refers to legal, sociological, technological, or legal aspects of crime and a universal definition remains elusive (Kshetri, 2010). Analysts have attempted to frame the fundamental characteristics of cyber-crime with limited consensus (Snyder, 2001; Williams, 2001; Wall & Yar, 2005; Gordon & Ford, 2006). Current definitions vary significantly, depending on the legal instrument or organization defining the term (Pocar, 2004). The abuse of ICTs by criminals is interchangeably referred to as cyber-crime, computer crime, computer misuse, computer-related crime, high technology crime, e-crime, technology-enabled crime, amongst others (Goodman & Brenner, 2002).

According to the ACPO, e-Crime involves the use of networked computer or Internet technology to commit or facilitate the commission of crime (Association of Chief Police Officers, 2009). Contrastingly, the AIC regards E-crime as A general label for offences

committed using an electronic data storage or communications device (Australian Institute of Criminology, 2011). The semantics of cyber-crime point to a legal and technical phenomenon that proscribes criminal activity connected with the cyber domain.

Evidence in judicial proceedings is increasingly being stored, transmitted, or processed in electronic form. Technology has become the symbol, subject (place), tool (instrument), and object (target) of crime (Savona & Mignone, 2004). Although technology facilitates the commission of traditional crimes, including offences against property and offences causing personal harm (McQuade, 2006), existing national legal frameworks may be incapable of addressing evolving '*modus operandi*' related to cyber-crime offending (Hughes, 2003).

It is common for cyber-crime to be transnational in terms of the physical location of victims, perpetrators, and evidence. The interconnectivity of the global economy enables criminals to operate trans-jurisdictionally, with discrete elements of their crimes speckled widely across the globe in both time and space (Herrera-Flanigan & Ghosh, 2010). Despite extra-territorial legal provisions for criminal acts perpetrated in foreign jurisdictions, the practical application of these laws is rather ineffective (Geist, 2003). Whilst an offender may be apprehended in one jurisdiction, the digital evidence required to progress an investigation may reside in another country (Scientific Working Group on Digital Evidence, 2000).

Ultimately, cyber-crime can be perpetrated inexpensively and easily, and victims are often left wondering if the offender is half a block or half a world away (Goodno, 2007). The anonymity of cyber-crime also increases the volume of offences and obstructs efforts to identify culprits, thereby distinguishing it from physical crimes (Brenner, 2008; Casey, 2004; Denning, 2001; Post, Ruby & Shaw, 2000). The disinhibiting effect of technology

serves to psychologically distance criminals from the consequences of their victimizing behaviour (Bocij & McFarlane, 2003; D'Ovidio & Doyle, 2003; Lidsky & Cotter, 2007). In addition to advanced technical aptitudes, cyber criminals have skills in linguistics and psychology, which they combine to execute social engineering deceptions, manipulate decision-making processes, and distort perceptions (Waltz, 1998; Mutnick & Simon, 2002; Holt, 2012; Chen, 2015).

It was reported in Romania that cyber criminals engage native English speakers to give a layer of legitimacy to online scams (Bhattacharjee, 2011). Compared to traditional criminal offences, cyber-crime requires fundamentally different strategic and tactical responses from legislators, investigators, lawyers, and judicial officers (Wall, 2001).

The relatively anonymous and faceless nature of cyber-crime complicates issues associated with victimology and cyber-crime reporting (Bermay & Godlove, 2012). There exists widespread misunderstanding among communities about the nature of cyber-crime and capacity of law enforcement to apprehend offenders. Many factors impact the low proportion of cyber-crime acts that are brought to the attention of police. There is also a widespread belief that law enforcement agencies are inflexible and intrusive (Davies, 1999; Wolf, 2000; Walden, 2005).

Victims fear that prosecutors will not take on their case, or if they do, will publicize the case widely to raise the profile of the prosecutor or department concerned, without due regard to the impact of such publicity on the victim (Shafritz, 2001; Spitzberg & Hoobler, 2002; Goodno, 2007; Herrera-Flanigan & Ghosh, 2010). This has resulted in most cyber-crimes not been investigated, and suspect apprehended. Many victims are also reluctant to come forward due to shame or the mistaken belief that the cyber-crime incident is simply

not serious enough to warrant police or investigator's attention (United Nations Office on Drugs and Crime, 2013).

Cyber-crime reporting and prosecution is also impeded by a lack of awareness regarding reporting mechanisms (United Nations Office on Drugs and Crime, 2013). Identifying victims and perpetrators of cyber-crime can be a very complex matter, and the disinclination of victims to come forward substantially impairs the capacity of police to respond. Widespread underreporting by Internet Service Providers (ISPs) indicates that new laws may be required to compel them to report suspicious activity on their networks (U.S. Department of Justice, 'A Review of the FBI's Investigations of Certain Domestic Advocacy Groups', 2010). Ultimately, the prevailing tendency for underreporting makes cyber-crime offences increasingly less visible even though they happen every day.

Organized and persistent cyber-attacks have circumvented security precautions within major global corporations and stolen information and money with relative ease (Robertson, Riley, Strohm & Chan, 2014). Advanced blended attacks leverage vulnerabilities in fixed and wireless networks to steal credentials and conduct reconnaissance (FireEye Labs, 2015). Criminals use behavioural profiling to masquerade as ordinary system users whilst navigating private networks and exploiting applications to avoid arousing suspicion (CrowdStrike, 2015). Ultimately, signature-based commercial solutions lack the intelligence needed to identify and neutralize persistent nefarious activity that moves laterally and quietly (Brown, 2015).

The idiom 'garbage in, garbage out' reflects the danger of appointing untrained and incapable personnel to capture proof of malicious activity and secure evidence of cyber-crime offences. Seasoned leadership is required to effectively direct investigations and supervise the provision of forensic support (Horswell, 2004; Raymond, 2006).

Unfortunately, bureaucrats with little in the way of technical background, often fill leadership positions in government, police, and law enforcement agencies within these areas. Like the organized criminal elements that embrace new technologies whilst adhering to proven techniques for committing crime, investigators must think like their criminal adversaries to decipher the technical underpinnings of cyber-crime offences (Nuth, 2008; Endgame, 2015).

Crime scene examiners are the essential of successful investigations and the critical first step for initiating the chain-of-custody (Stanley & Horswell, 2004). Technology improves the capacity of investigator to capture a vast array of potential evidence (Mandel, 1987), but it is the human side of a cyber-crime inquiry which is pivotal for giving meaning and weighing significance for prosecution and conviction. Investigators must interpret and correlate information to support case theories and pursue leads by initiating dialogues with key individuals that are central to an investigation. It is critical for law enforcement agencies to retain personnel with this investigative mindset to expose cyber-crime offences. Aside from electronic evidence, investigators also draw on other forensic science disciplines to gather physical trace evidence from crime scenes, including print, hair, and fiber artifacts (Kaye, 1995; Gilbert, 2004; White, 2004).

Prior to commencing a search, investigators must ensure that they abide by applicable laws or risk having seized exhibits declared inadmissible at trial. In some jurisdictions, there are exceptions that may justify warrantless search and seizure activities (e.g., consent, ‘emergency’ terrorist situations, plain view doctrine, search relating to arrest, etc.) but an actual search of the data stored on a device usually requires a warrant in common law countries. In circumstances where there is a substantial risk of losing evidence, such as where data sanitizing and other anti-forensics tools are active, some

jurisdictions permit law enforcement to perform a limited search of devices without a warrant due to the perceived vulnerability of the data (Dee, 2012).

Many law enforcement agencies have developed specialized units that target offenders online through social networking websites, chat rooms, instant messaging platforms, cloud services, Darknet forums, and other peer-to-peer communicative mediums (Mitchell, Wolak & Finkelhor, 2005; Dubord, 2008). Undercover operatives conducting online investigations use the trick of impersonation in an attempt to build trust from targeted suspects. In many cases, online investigations are initiated further to complaints received from parents in circumstances where someone has contacted a child online and is behaving inappropriately (Tetzlaff-Bemiller, 2011). Such investigations are reactive and may involve an undercover officer taking control of a child's online identity to discover more about the intentions of a suspect (Mitchell, Wolak & Finkelhor, 2005).

By interacting directly with suspects, investigators can witness offences as they occur and need only wait for perpetrators to reveal themselves (Girodo, Deck & Morrison, 2002, Tetzlaff-Bemiller, 2011). For the most part, this type of undercover work targets criminals involved in child sex solicitation and abuse. However, with the emergence of highly organized online criminal marketplaces, the scope of online offences is now vast (e.g., drug trafficking, contract killing, trading in stolen credit cards, malware distribution, money laundering, etc.) (Lusthaus, 2013). Investigators engaged in undercover operations require a comprehensive understanding of the laws governing engagement with suspects to ensure the admissibility of evidence and credibility of admissions (e.g., entrapment, inducement, etc.) (Ballin & Ballin, 2012). Proactive investigations of this nature often succeed because the problem of attributing criminal activity online also makes it very difficult for offenders to identify undercover agents (Lusthaus, 2012).

Personal, public and private domains are increasingly interconnected through networked infrastructure, ranging from a small number of devices connected in close proximity to literally thousands of devices linked through virtual private networks that span geographical and jurisdictional boundaries (Smith, 2004; Zatyko & Bay, 2011). The popularity of cloud computing has amplified cross-border investigative and privacy issues because domestic laws are innately local and the cloud is intrinsically global. Inside their data centers, cloud service providers (CSPs) offer access to powerful computing and networking infrastructure (Grace & Mell, 2011). Resources are delivered to users as a service that is accessed remotely over a network. The service offerings are distinguished according to functionality and delivery model. Cloud computing is a force multiplier and the expanding consumer base globally offers cyber criminals both a centralized pool of victims as well as new avenues to exploit digital resources and evade detection (Mills, 2012). Cloud services may become the target of criminal activity (e.g., unauthorized access, system sabotage, data theft, spying/stalking, etc.). In the same vein, Cloud services may also be leveraged as a means of committing criminal activity. Network Forensic is therefore a way to go to discover, detect, and better still prevent all cyber related crimes.

2.3 Theoretical Framework

2.3.1 Rational Choice Crime Theory

For rational choice theorists, a criminal rationally chooses the crime to commit and the target of crime (Clarke, 1987). A recent reformulation and integration of earlier classical and positivist theory is found in rational choice theory. Developed by Derek Cornish and Ronald Clarke, rational choice theory focuses on the situational aspects of criminal behaviour. Rational choice (or situational) theory stresses the point that society can achieve a high degree of crime detection by focusing on the situational aspects that influence particular types of criminal behaviour and consequently committing crime. As per the rational choice theory,

a criminal rationally chooses both the crime to commit and the target of the crime (Cornish & Clarke, 1986). In other words, the criminal, does not randomly select his or her target.

2.3.2 Deterrence Theory

Deterrence theory suggests that an individual's choice to commit or not commit a crime is influenced by the fear of punishment. Deterrence is the act of preventing a criminal act before it occurs, through the threat of punishment and sanctions. Rooted in the classical perspective, deterrence theory focuses on the following premises:

i. For punishment to be a deterrent to criminal behaviour, it must be certain, swift, and severe.

ii. The severity must be sufficient to outweigh any rewards that the criminal may obtain from a criminal act.

The crime rates should decline if there is an increase in the rates of arrest, conviction, and severity of punishment due to the deterrent effect. Deterrence theory includes the idea that forced retribution for a crime should reduce crime rates. Retribution is the notion that a wrongdoer should be forced to pay back or compensate for his or her criminal acts. During the 1970s and into the 1980s, there was a return to Retributivism in the justice model. The concept of just deserts is the pivotal basis of the justice model. Just deserts are a justice perspective which provides that whoever violate others rights deserves to be punished. The severity of the punishment should also be commensurate with the seriousness of the crime. In addition to returning to the justice model, the United States in the 1970s and 1980s reverted to a utilitarian punishment philosophy to deal with crime.

2.3.3 Cesare Beccaria Classical Theory of Crime

Beccaria considered that criminals owe a debt to society and proposed that punishments should be fixed strictly in proportion to the seriousness of the crime. Torture was considered a useless method of criminal investigation, as well as being barbaric. Moreover, capital

punishment was unnecessary with a life sentence of hard labour preferable, both as a punishment and deterrent. The use of imprisonment should thus be greatly extended, the conditions of prisons improved with better physical care provided and inmates should be segregated on the basis of gender, age and degree of criminality. Beccaria was a very strong supporter of 'social contract' theory with its emphasis on the notion that individuals can only be legitimately bound to society if they have given their consent to the societal arrangements. It is nevertheless the law that provides the necessary conditions for the social contract and punishment exists only to defend the liberties of individuals against those who would interfere with them. Beccaria's theory of criminal behaviour is based on the concepts of free will and hedonism where it is proposed that all human behaviour is essentially purposive and based on the pleasure-pain principle (Beccaria, 1963).

2.3.4 Routine Activities Theory (RAT)

Routine activities theory stresses the idea that criminals balance the costs and benefits of committing crimes. Classical theorists explain crime as a rational course of action by offenders who seek to minimize pain and maximize pleasure. Routine activities theory is a product of the classical approach. Routine activities theory (RAT) stresses the idea that criminals are not impulsive or unpredictable, because they balance the costs as well as benefits of committing crimes (Felson & Clarke, 1998). In an analysis of crime and routine activities, Lawrence E. Cohen and Marcus Felson consider the trends in crime rates in terms of the changing routine activities of everyday life. RAT explains why crime and delinquency occur in particular places under specific conditions. It does this by focusing on the convergence of motivated offenders, suitable targets, and the absence of capable guardians against a violation. RAT assumes that-

i. Self-interest motivates criminal offenders to commit criminal acts;

ii. Many individuals may be motivated to break laws.

Suitable targets may be valued (e.g., jewellery, cars, or cash) or people who, when assaulted, provide positive rewards or pleasure to the perpetrator. Guardians are defined as objects (e.g. gates, surveillance cameras, or burglar or auto alarms) or individuals (e.g., guards or police) who can protect possible targets or victims. To the offender, the presence of protective guardians raises crime costs and lessens target attractiveness. RAT studies focus on direct-contact predatory violations—illegal acts in which someone definitely and intentionally takes or damages the person or property of another. Focusing on crime events and not on criminal offenders themselves, RAT examines how structural changes in everyday activity patterns influence crime rates by affecting the convergence in time and space of three requisite conditions for a crime to occur. These three conditions include-

i. A perpetrator;
ii. A victim and/or an object of property (criminal victimization increases when motivated offenders and targets converge);
iii. A relationship or an opportunity (criminal victimization decreases with the presence of capable guardians).

2.3.5 Agnew's Strain Crime Theory

In response to studies that had failed to support traditional strain theory's core proposition that the inability to achieve desired goals such as middle-class status or economic success would motivate adolescents to engage in delinquency, Agnew (1992) extended classic strain theory by focusing on other possible sources of strain (defined as events or conditions that are disliked by individuals (Agnew, 2006, p. 4)). Instead of one general strain-producing source, Agnew identified three major sources: 1) the failure to achieve positively valued goals, including the disjunction between expectations and actual outcomes and the perception of what would be a fair or just outcome and actual outcomes; 2) the removal (or threat of removal) of positively valued stimuli that the actor already possesses (e.g., the death of a

parent or the loss of a girlfriend); and 3) presentation with noxious or negatively valued stimuli, such as abuse.

Agnew argued that much of this strain originates from negative relationships that the person has with others and the negative emotions (both emotional states and traits, with the latter being linked to cumulative exposure to strains) such as anger, frustration, and resentment that result from these relationships. The corrective response to these negative emotions may take the form of crime (especially when the costs of crime are relatively low, the individual is experiencing low levels of social control, and the individual is disposed to commit crime; Agnew, 2006), with the behavioural solution being instrumental (get back what one lost), retaliatory (strike out against the perceived cause of the stress), or escapist (e.g., engage in substance use to alleviate the displeasure from the negative emotional state) in nature. One can manage these strains legitimately if the actor has effective coping mechanisms, however. Such moderating variables include one's self-concept, one's level of social support, mastery and problem-solving skills (Agnew, 1992).

He also argued that individuals who are self-efficacious, who have extensive social support networks, and who have a positive self-concept are less likely to resort to crime or deviance in response to exposure to strains. In addition, the inclination of one's peers towards (or against) deviance can affect whether an individual is likely to turn to crime in response to strain (although chronic exposure to strain increases the likelihood that an individual will join with criminal others; Agnew, 2006, p. 43). Thus, explaining crime involves not only the level of exposure to strains but also the extent and type of coping mechanisms available to the individual and the individual's peer associations.

2.3.6 General Strain Crime Theory

While general strain crime theory can help make sense of the peak in crime and deviant activity in adolescence for many offenders, it can also be used to explain persistence versus desistance from crime in young adulthood. Although it is a core dimension of life course criminology, research into the correlates of such processes is relatively limited (Loeber & LeBlanc, 1990; Piquero, Farrington, & Blumstein, 2003; Gunnison & Mazerolle, 2007; Kazemian, 2007). Laub and Sampson (2001), in a comprehensive review of the issue, have noted that conceptual, definitional, and measurement issues have limited research exploring the issues of desistance and persistence, despite its importance in developmental criminology. At the conceptual level, the notion of desistance is problematic because, as Maruna wrote, desistance from crime is an unusual dependent variable for criminologists because it is not an event that happens, but rather it is the sustained absence of a certain type of event (in this case, crime) (2001, p.17; as quoted in Laub & Sampson, 2001, p. 5). Furthermore, the causes of desistance are simply the opposites of the causes of onset of criminal behaviour (Gottfredson & Hirschi, 1990), or if there exist notable distinctions in the correlates of each (Farrington, 1992; Uggen & Piliavin, 1998). Additionally, many scholars have noted that there is no agreed upon definition of desistance (Bushway, Piquero, Broidy, Cauffman & Mazerolle, 2001; Laub & Sampson, 2001; Piquero, Farrington, & Blumstein, 2003; Kazemian, 2007).

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Research Design

For this research, descriptive research design was used. The descriptive design describes phenomena as they exist. It was used to identify and obtain information on the characteristics of a problem or issue. Descriptive research design was selected because it has advantage of producing good amount of responses from a wide range of people. It also deals with collecting and measuring of data in countable form, for example, test scores, Likert scales, reaction time and so on (Hammond & Wellington, 2013). Also, this design provides a meaningful and accurate picture of events and seeks to explain people's perception and behaviour based on the data collected.

3.2 Population and Sampling Techniques

The target population for this study is 49 comprising staff of the Counter-terrorism and General Investigation Unit of the Economic and Financial Crimes Commission(EFCC) who work in the Forensic Laboratory, staff of the department of Asset Tracing and Recovery Management and Intelligence Security and Support of Independent Corrupt Practices and Other Related Offences Commission(ICPC) who also work with the Forensic Laboratory, and staff of the Investigation Department Nigerian Police Force(NPF) who were Digital Forensic experts and work in the Forensic Laboratory and are based in the Federal Capital Territory office.

For this study, I adopted the census survey because of the population size which was small. Census survey involves complete listing of all the samples in each population. Census survey is studying the entire population as the sample size. There are conditions that warranted the

study of the entire population, one of which was if the entire population was small (Nwana, 2005).

Census survey was used because the population size is small. Table 3.1, shows the selected sample from each agency.

Table 3.1: Selected Samples per Agency

Name of Agency	Department/Unit	Number of Sample/Staff
EFCC	Counter-terrorism and General Investigation	24
ICPC	Asset Tracing and Recovery Management and Intelligence Security and Support	11
NPF	Investigation	14
	Total	49

Source: Field Survey, 2018

3.3 Method of Data Collection

Questionnaire was used as instrument in data collection and the respondents were required to read each question carefully and indicate their agreement or disagreement with the statement using a 5 point Likert scale which was scaled ranging from: 5 = “strongly agree”, 4 = “agree”, 3 = “undecided”, 2 = “disagree”, and 1 = “strongly disagree”.

3.3.1 Validity of Survey Instruments

Academic professionals and experts from the Institute of Corporate Governance and Development Studies (Prof. Akinwumi, and Dr Abdul Adamu) of Nasarawa State University, Keffi reviewed the survey instrument for content and face validity. The comments and suggestions of my supervisor and these experts were used to revise the instrument such that

the objectives of this research were covered. The researcher also administered the questionnaires to selected respondents who are not included in the population to ensure that the questions were easily understood and hold the same meaning to all the respondents.

3.3.2 Reliability Test

For this research, the most convenient method that was used for testing internal consistency is the Cronbach's Alpha. Several studies recommended acceptable values of alphas ranging from 0.68 to 0.95 (Bryman, 2004), with Cronbach's Alpha value of 0.60 as the minimum acceptable. Consequently, the Cronbach's alpha reliability estimates for the variables measuring the effect of Digital Forensic on Crime detection in this research's instrument were as shown in Table 3.2 below. These values are derived using this formula: $\alpha = \frac{Nr}{1+r(N-1)}$

Where:

α = Cronbach's alpha

N = the number of items in the scale

r = the mean inter-item correlation

Table 3.2: Reliability Estimates for the Measure of Digital Forensic on Crime Detection

Constructs	Number of Questions	Cronbach's alpha
Computer Forensic and Crime Detection	5	α = 0.84
Mobile Forensic and Crime Detection	4	α = 0.82
Network Forensic and Crime Detection	4	α = 0.82
Crime Detection	5	α = 0.84

3.4 Technique for Data Analysis and Model Specification

Given the nature of the survey, and the objectives of the study, the multiple regression technique of data analysis was adopted. A descriptive analysis was used, with cross tabulations used to represent all variables. Cross-sectional regression analysis usually follows a pattern of model development for testing moderation as suggested by Creswell (2009). The

model tested the direct relationship between the dependent variable – Crime Detection, and the proxies of the independent variables which are Computer Forensic, Mobile Forensic, and Network Forensic to establish the unconditional relationship between the variables. This model is as represented in the functional equation below:

Crime Detection = f(Computer forensic, Mobile forensic, and Network forensic)

$$CD_i = \alpha_0 + \beta_1 CF_i + \beta_2 MF_i + \beta_3 NF_i + \mathcal{E}_i \ldots\ldots\ldots \textit{Equ. (1)}$$

3.4.1 Variable Measurement

The variables that were used in this study as proxies of the concepts under investigation are measured in the survey instrument as presented in Table 3.3 below:

Table 3.3: Variable Measurement

Variable Name	Acronym	Measurement
Crime Detection	CD	5 point Likert scale based on survey instrument
Computer Forensic	CF	5 point Likert scale based on survey instrument
Mobile Forensic	MF	5 point Likert scale based on survey instrument
Network Forensic	NF	5 point Likert scale based on survey instrument
Constant	A	
Coefficient	B	
Error term	Ɛ	

Source: Author's Research Definition

3.5 Justification of Methods to be used

Descriptive analysis was used to explain each question posed in the questionnaire to better explain the position of the respondents as regards the effect of Computer Forensic, Mobile Forensic, and Network Forensic. Also, Multiple regression analysis was used because it is efficient in ascertaining the relationship between research variables and adequately analysing phenomena. In this case, the dependent variable which is crime detection was tested to

determine if Computer Forensic, Mobile Forensic, and Network Forensic have significant effect on it. The Statistical Packages for Social Sciences (SPSS) was used in achieving this.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.1 Data Presentation

This chapter presents the analysis of the data collected from the field and the discussion of the results. Primary data were collected on the effects of Digital Forensic on Crime Detection in Nigeria. This study is a census survey hence, the total population of the study was 49 staff drawn from 3 law enforcement agency namely EFCC, ICPC, and NPF. These staff works with their various forensic department or laboratory. Therefore, a total of 49 copies of questionnaires were distributed to all the staff. The entire questionnaires were correctly filled and returned giving a response rate of 100%. The data is presented in the appendix II.

4.1.1 Presentation of General Information

This section provides general information on the respondents of this study. These include, the agency, their years of experience in Digital Forensic, and level of Education.

4.1.1.1 Name of Agency

Table 4.1: Name of Agency

Name of your Agency					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	EFCC	24	49.0	49.0	49.0
	ICPC	11	22.4	22.4	71.4
	NPF	14	28.6	28.6	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

From Table 4.1 above, a total of 49% are staff of EFCC while ICPC and NPF are 22.4% and 28.6% respectively. This shows that EFCC have more staff that specialised in Digital forensic.

4.1.1.2 Years of Experience is Digital Forensic

Table 4.2 below shows that more staff of the 3 agencies has their experience falls within 4 to 7 years with 63.3%, followed by those with 1 to 3 years with 24.5%p, and those with 7 years and above are just 12.2%.

Table 4.2: Years of Experience

Years of Experience in Digital Forensics (Years)					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-3years	12	24.5	24.5	24.5
	4-7years	31	63.3	63.3	87.8
	More than 7years	6	12.2	12.2	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.1.3 Level of Education

Table 4.3: Level of Education

Level of Education					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Graduate(Bachelor's/HND)	40	81.6	81.6	81.6
	Postgraduate(PGD/MSc/PhD)	9	18.4	18.4	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

From table 4.3 above, it was observed that 81.6% of the respondents are graduates while a total of 9 respondents with 18.4% hold a postgraduate degree. This simple means that all the respondents hold at least a bachelor's degree or Higher National Diploma.

4.1.2 Computer Forensic and Crime Detection

This section discussed major principles involved in Computer forensic and it revolves around the basic steps taken in a Computer forensic laboratory or domain. These are explained in the tables below.

4.1.2.1 General Computer Forensic Procedures

Table 4.4: General Computer Forensic Procedures

I follow all general Computer Forensic procedure and principles while identifying and collecting digital evidence					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	2.0	2.0	2.0
	Disagree	2	4.1	4.1	6.1
	Undecided	2	4.1	4.1	10.2
	Agree	16	32.7	32.7	42.9
	Strongly Agree	28	57.1	57.1	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

It was observed from table 4.4 above that a total of 89.8% of the respondents do follow all general Computer forensic procedure and principles while identifying and collecting digital evidence. Meanwhile, 4.1% could not decide and 6.1% disagree.

4.1.2.2 Evidence and its Integrity

Table 4.5 below shows that about 79.6% of the respondents ensure that action taken on evidence do not alter its integrity. While 4.1% are undecided, 16.3% disagrees; this shows that there could be some margin of error.

Table 4.5: Evidence and its Integrity

I ensure action taken do not change evidence and its integrity are kept intact					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	4.1	4.1	4.1
	Disagree	6	12.2	12.2	16.3
	Undecided	2	4.1	4.1	20.4
	Agree	14	28.6	28.6	49.0
	Strongly Agree	25	51.0	51.0	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.2.3 Evidences Analysed without Modification

Table 4.6 below depicts the percentages of those that ensure all evidences collected are analysed without modifying them to be 85.7%. The remaining 14.3% either undecided or disagree.

Table 4.6: Evidences Analysed without Modification

I ensure all evidences collected are analyzed without modifying them					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	4.1	4.1	4.1
	Disagree	1	2.0	2.0	6.1
	Undecided	4	8.2	8.2	14.3
	Agree	18	36.7	36.7	51.0
	Strongly Agree	24	49.0	49.0	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.2.4 Activities fully Documented, Preserved, and available for Review

This focuses on adequate maintenance of chain of custody. This is a vital and integral part of forensic process. From Table 4.7 below, 73.5% agrees to this while 16.3% disagrees and 10.2% were undecided.

Table 4.7: Activities fully Documented, Preserved and available for Review

All activities related to seizure, access, storage or transfer of evidence are fully documented, preserved and available for review					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	4.1	4.1	4.1
	Disagree	6	12.2	12.2	16.3
	Undecided	5	10.2	10.2	26.5
	Agree	15	30.6	30.6	57.1
	Strongly Agree	21	42.9	42.9	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.2.5 Legally Justifiable Methods and Techniques

The choice of methods and techniques are very important in Computer Forensic as there might be different alternatives that might not provide adequate results. From table 4.8 below, a total of 87.7% admits to using approved methods and techniques. On the other hand, 10.2% disagrees while 2% were undecided.

Table 4.8: Legally Justifiable Methods and Techniques

I ensure that legally justifiable methods and techniques are used to derive useful information that address the crime committed					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	2.0	2.0	2.0
	Disagree	4	8.2	8.2	10.2
	Undecided	1	2.0	2.0	12.2
	Agree	11	22.4	22.4	34.7
	Strongly Agree	32	65.3	65.3	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.3 Mobile Forensic and Crime Detection

This section discussed findings from the research that involved Mobile forensic. These are explained in the tables below.

4.1.3.1 Protecting the Volatility nature of Phone Evidence

From Table 4.9 below, 69.4% of respondents ensure that adequate measures are taken to protect the volatility nature of phone and mobile evidences while 12.2% does not consider this as an issue and 18.4% are undecided.

Table 4.9: Protecting the Volatility nature of Phone Evidence

I ensure that adequate measures are taken to protect the volatility nature of Phone evidence					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	2.0	2.0	2.0
	Disagree	5	10.2	10.2	12.2
	Undecided	9	18.4	18.4	30.6
	Agree	14	28.6	28.6	59.2
	Strongly Agree	20	40.8	40.8	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.3.2 Actors, Actions, and State of Interest of a Crime

Table 4.10 below detailed the percentages of respondents that considered and ensure standard procedures are taken while identifying actors, actions, and the state of interest of a crime. 75.5% of respondents ensures this is done while 20.4% disagrees and 4.1% undecided.

Table 4.10: Actors, Actions, and State of Interest of a Crime

In identifying actors, actions, and state of interest of a crime, I ensure that standard procedures are taken					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	4.1	4.1	4.1
	Disagree	8	16.3	16.3	20.4
	Undecided	2	4.1	4.1	24.5
	Agree	8	16.3	16.3	40.8
	Strongly Agree	29	59.2	59.2	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.3.3 Anti-forensic check on Mobile devices

Table 4.11: Anti-forensic check on Mobile devices

I ensure I do a proper anti-forensic check in Mobile devices while collecting and analysing evidence					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	7	14.3	14.3	14.3
	Disagree	10	20.4	20.4	34.7
	Undecided	4	8.2	8.2	42.9
	Agree	12	24.5	24.5	67.3
	Strongly Agree	16	32.7	32.7	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

Table 4.11 above depicts the percentage of respondents that ensure to do proper anti-forensic check in mobile devices while collecting and analysing evidence. 57.2% agrees to this while 34.7% does not with 8.2% undecided.

4.1.3.4 Link Analysis

Table 4.12: Link Analysis

I ensure a proper link analysis is done at the analysis phase to determine the extent of Crime and to validate the purpose of Investigation					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	4.1	4.1	4.1
	Disagree	2	4.1	4.1	38.8
	Undecided	6	12.2	12.2	34.7
	Agree	9	18.4	18.4	22.4
	Strongly Agree	30	61.2	61.2	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

Table 4.12 above shows the frequencies and percentages of respondents that ensure that a proper link analysis is done at the analysis phase to determine the extent of crime and to validate the purpose of investigation. 79.6% agrees that this is properly done while 8.2% disagrees. 12.2% could not decide whether they do this or not.

4.1.4 Network Forensic and Crime Detection

This section discussed findings from the research that involved Network forensic. These are explained in the tables below.

4.1.4.1 Evidences collected through Network Packets

Here, respondents were asked if they ensure that all evidences related to network activities are collected through Network Packets, firewall logs, Intrusion Detection Systems logs, System logs, routers log and audit logs in determining the nature of crime. As shown on table 4.13, 67.3% respondents support this, while 26.5% of the respondents disagree. 6.1% of the respondents were undecided.

Table 4.13: Evidences collected through Network Packets

I ensure that evidences are collected through Network Packets, firewall logs, IDS logs, system logs, routers log and audit logs depending on the nature of Crime					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	10	20.4	20.4	20.4
	Disagree	3	6.1	6.1	26.5
	Undecided	3	6.1	6.1	32.7
	Agree	15	30.6	30.6	63.3
	Strongly Agree	18	36.7	36.7	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.4.2 Adequate attention to Anti-forensic techniques

Table 4.14 below detailed the responses gathered from 49 respondents on whether they pay adequate attention to anti-forensic techniques such as Data and IP hiding, Data destruction while acquiring evidence. 77.6% agrees to this while 10.2% of the respondents disagree. 12.2 % of the respondents were undecided.

Table 4.14: Adequate attention to Anti-forensic techniques

I pay adequate attention to anti-forensics techniques (Data hiding, IP hiding, Data Destruction etc) while acquiring evidence					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	2.0	2.0	2.0
	Disagree	4	8.2	8.2	10.2
	Undecided	6	12.2	12.2	22.4
	Agree	17	34.7	34.7	57.1
	Strongly Agree	21	42.9	42.9	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.4.3 Evidences Validated in every step taken

Table 4.15: Evidences Validated in every step taken

I ensure that evidences are validated in every step taken in analysis					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	2.0	2.0	2.0
	Disagree	4	8.2	8.2	10.2
	Undecided	2	4.1	4.1	14.3
	Agree	14	28.6	28.6	42.9
	Strongly Agree	28	57.1	57.1	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

Above is table 4.15 that shows respondents responses to how they ensure that evidences are validated in every step taken in analysis. 85.7% of the respondents agree while 10.2% disagree.

4.1.4.4 Integrity of Evidence

Table 4.16: Integrity of Evidence

To protect the integrity of evidence, I ensure that all deleted files from all sources are recovered for the Investigation					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	12.2	12.2	12.2
	Disagree	7	14.3	14.3	26.5
	Undecided	2	4.1	4.1	30.6
	Agree	18	36.7	36.7	67.3
	Strongly Agree	16	32.7	32.7	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

On table 4.16 above, respondents gave their responses on the recovery of deleted files from all sources of evidence in an investigation in other to protect its integrity. 69.4% of respondents agree while 26.5% of respondents disagree. 4.1% of respondents were undecided.

4.1.5 Crime Detection

In this section, aspects of Digital forensic were looked at with a view of knowing how they affect crime detection.

4.1.5.1 Computer forensic has helped in Crime detection

Table 4.17: Computer forensic has helped in Crime detection

Computer Forensic has helped in detecting more crime than the traditional Investigation methods based on my experience					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	4.1	4.1	4.1
	Disagree	6	12.2	12.2	16.3
	Undecided	5	10.2	10.2	26.5
	Agree	7	14.3	14.3	40.8
	Strongly Agree	29	59.2	59.2	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

The question posed here to determine if Computer forensic has helped in detecting more crime than the traditional investigation methods based on the respondents experience.

73.5% of the respondents agree to this while 16.3% of the respondents disagree. 10.2% of the respondents were undecided.

4.1.5.2 Mobile forensic has helped in Crime detection

On table 4.18 below, respondents were asked if Mobile forensic has helped in recording more success in Crime detection. 71.4% of the respondents agree while 16.3% of the respondents disagree. 12.2% of the respondents were undecided.

Table 4.18: Mobile forensic has helped in Crime detection

More success has been recorded in Crime Detection with Mobile Forensic					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	7	14.3	14.3	14.3
	Disagree	1	2.0	2.0	16.3
	Undecided	6	12.2	12.2	28.6
	Agree	17	34.7	34.7	63.3
	Strongly Agree	18	36.7	36.7	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.5.3 Network Forensic has helped in Crime detection

Table 4.19: Network Forensic has helped in Crime detection

Network Forensic has helped greatly in resolving the anonymous nature of Network attack which usually poses challenge in Crime Detection					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	6.1	6.1	6.1
	Disagree	9	18.4	18.4	49.0
	Undecided	2	4.1	4.1	30.6
	Agree	10	20.4	20.4	26.5
	Strongly Agree	25	51.0	51.0	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

Network forensic has helped greatly in resolving the anonymous nature of Network attack which usually poses challenge in Crime detection was the question put forward here. 71.4% of respondents agree that Network forensic has helped in crime detection while 24.5% of respondents disagree. 4.1% of respondents were undecided.

4.1.5.4: Forensic has increased prosecution of Crimes

Table 4.20 below depicts responses from respondents on whether prosecution of crime has increased because of forensic activities or not. 65.3% of respondents agree while 26.5% of respondents disagree. This shows that forensic has increased prosecution of crimes.

Table 4.20: Forensic has increased prosecution of Crimes

Prosecution of crime has increased because of Forensic activities					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	6	12.2	12.2	12.2
	Disagree	7	14.3	14.3	26.5
	Undecided	4	8.2	8.2	34.7
	Agree	11	22.4	22.4	57.1
	Strongly Agree	21	42.9	42.9	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

4.1.5.5 Relevant laws made digital forensic acceptable in court

Table 4.21: Relevant laws made digital forensic acceptable in court

The Cyber Crime Act 2015 and Evidence Act 2011 have form part of the basics for the acceptance of all our evidences in criminal and administrative cases					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	9	18.4	18.4	18.4
	Disagree	5	10.2	10.2	28.6
	Undecided	6	12.2	12.2	40.8
	Agree	6	12.2	12.2	53.1
	Strongly Agree	23	46.9	46.9	100.0
	Total	49	100.0	100.0	

Source: Field survey, 2018.

The Cyber Crime Act 2015 and Evidence Act 2011 (as amended) have form part of the basics for the acceptance of all digital evidences in criminal and administrative cases was the questions here, 59.1% of respondents supported this while 28.6% disagrees. 12.2% of respondents were undecided.

4.2 Data Analysis and Results

Table 4.22: Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.536[a]	.287	.240	4.75726
a. Predictors: (Constant), NF, CF, MF				

Source: Field survey, 2018.

Table 4.22 above shows the summarized regression, it shows the value of R of 0.536 that is, 53.6%. This shows significant relationship between the dependent variable (Crime Detection) and the independent variables (Computer Forensic, Mobile Forensic and Network Forensic).

The R^2 value of 0.287 reveals that 28.7% of changes or variation that occurred in Crime Detection is attributed to Computer Forensic, Mobile Forensic and Network Forensic.

Table 4.23: Analysis of Variance

ANOVA[b]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	410.400	3	136.800	6.045	.002[a]
	Residual	1018.417	45	22.631		
	Total	1428.816	48			
a. Predictors: (Constant), NF, CF, MF						
b. Dependent Variable: CD						

Source: Field survey, 2018.

From table 4.23 above, the significant value (Sig. value) of 0.002 is less than 0.05 level of significance, which implies that the overall regression model is statistically significant, that is, the overall model is fit for prediction. The regression model result implies that all independent variables are highly significant in explaining that there is a significant relationship between the dependent variable and independent variables.

Table 4.24: Correlations Matrix

		CD	CF	MF	NF
CD	Pearson Correlation	1	-.356*	-.111	.302*
	Sig. (2-tailed)		.012	.448	.035
	N	49	49	49	49
CF	Pearson Correlation	-.356*	1	.605**	.240
	Sig. (2-tailed)	.012		.000	.097
	N	49	49	49	49
MF	Pearson Correlation	-.111	.605**	1	.461**
	Sig. (2-tailed)	.448	.000		.001
	N	49	49	49	49
NF	Pearson Correlation	.302*	.240	.461**	1
	Sig. (2-tailed)	.035	.097	.001	
	N	49	49	49	49

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

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

Source: Field Survey, 2018.

Correlations were computed among four variables, that is, Crime Detection, Computer Forensic, Mobile Forensic and Network Forensic for 49 respondents. The results suggest that Computer Forensic and Network Forensic were statistically significant with Crime Detection. There values are given to be $r(49) = 0.356$, $p < .05$ and $r(49) = 0.302$, $p < .05$ in a two-tailed

test respectively. The correlations of Mobile Forensic with Computer Forensic, Network Forensic with Mobile Forensic, Mobile Forensic with Crime Detection and Network Forensic with Computer Forensic were not significant. There values are given to be $r(46) = 0.605$, $p < .01$, $r(46) = 0.461$, $p < .01$, $r(46) = -0.111$, $p < .01$ and $r(46) = 0.240$, $p < .01$ in a two-tailed test respectively. In general, the results suggest that Computer Forensic and Network Forensic tend to relate more with Crime Detection, than Mobile Forensic.

Table 4.25: Regression Result

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	27.027	5.331		5.070	.000
	CF	.783	.289	.429	2.710	.009
	MF	.064	.227	.549	4.281	.001
	NF	.610	.202	.428	3.011	.004
a. Dependent Variable: CD						

Source: Field survey, 2018.

4.2.1 Test of Hypotheses

For this study, three hypotheses were proposed and are therefore tested below in relation to the multiple regression result in table 4.25.

H_{01}: Computer Forensics do not significantly affect Crime Detection in Nigeria

From table 4.25 above, Computer Forensic has a positive contribution on Crime Detection. The P-value of 0.009 indicated that Computer Forensic is significant at 5% (0.05) level of significance, which means that Computer Forensic significantly affect Crime Detection. Therefore, this answers the first hypothesis by rejecting the null which states that Computer Forensics do not significantly affect Crime Detection, and accepting the alternative hypothesis which states that Computer forensics significantly affect Crime Detection.

H_{02}: Mobile Forensics do not significantly affect Crime Detection in Nigeria

Similarly, from table 4.25, Mobile Forensic has a positive relationship with Crime Detection. Mobile Forensic is one of the major contributors to Crime Detection due to the fact that it's P-value of 0.001 shows that it is significant at 5% level of significance. This answers the second hypothesis by rejecting the null which states that Mobile Forensics do not significantly affect Crime Detection and accepting the alternative hypothesis which is Mobile forensic significantly affect Crime Detection.

H_{03}: Network Forensics do not significantly affect Crime Detection in Nigeria

Also from table 4.25, Network Forensic also has positive contribution on Crime Detection. The P-value of 0.004 indicates that Network Forensic is significant to Crime Detection, also this answers the third hypothesis by rejecting the null which states that Network Forensics do not significantly affect Crime Detection and accepting the alternative hypothesis which state that Network forensic significantly affect Crime Detection.

4.3 Discussion of findings

The study result of analysis revealed that Digital forensic significantly affect Crime detection. This resulted from the test of hypothesis for the effect of Computer forensic, Mobile forensic, and Network forensic on Crime detection. The study emphasized that Computer forensic significantly affect crime detection. This study support the work of Samanthi and Sunesh (2016) that Computer forensics discloses content of emails, metadata associated with files related to Crime with the possibility of revealing documents related to the crime, the day it was created and last modified, and which user has done these actions.

Based on the data analysed and the hypothesis tested, it is evident that Computer forensic has helped significantly in the detection of Crime. Most of the respondents also agreed that Computer forensic has helped in detecting more crime than the traditional investigation

methods. This result is in line with the findings of Simms and Petersen(1991); Rooyen(1994); Lushbaugh & Wells(2000); Stephenson(2000); Joubert(2001); Taylor(2003); Bennett and Hess(2004); Callagher & Aro(2005); Skalak & Clayton(2006).

The study also revealed that Mobile forensic significantly affect Crime detection. This is in line with the findings of Cardwell et al(2007) who reported that investigator obtain electronic evidence in order to link a suspect to a Crime and subsequently prosecution. The survey result revealed that law enforcement employee agreed that they follow the right procedures in achieving high rate of criminal prosecution by identifying actors, actions, and state of interest of a Crime and also ensure proper measures are taken in the collection and analysis of evidence towards prosecuting a Crime. Such Crime according to Van Rooyen (2004) may include corruption, fraud, embezzlement, and white-collar related. Respondents also agreed that more success has been recorded in Crime detection by applying Mobile forensic which provides scientifically reputable repeatable evidence to secure prosecution; this is also in line with the conclusion of Satish et al. (2016).

The findings from the study also reveals that Network forensic has a significant effect on Crime detection. This involves monitoring network traffic and event to determine if there are anomalies that indicates an attack which required investigation and subsequently prosecution. This is in line with the work of Ranum (2012). Most of the respondents agreed that in order for the integrity of evidence to be maintained, they ensure that all deleted files from all network sources are recovered for all network related cases which are transnational organised crime according to Clapper (2015). From the responses in this study that emphasised that Network forensic has helped greatly in resolving the anonymous transnational nature of Network attack that usually poses challenge in Crime detection, this is in support of the study of Broadhurst et al. (2014); Kaspersky Lab (2015) and Ponemon Institute (2015). This contradict the conclusions of Zavrsnik (2010); Frolova (2011) and Onyshikiv and

Bondarev(2012) and that says that many investigations and prosecutions are failing to get off the ground in relation to Network forensic.

The findings also reveal that all respondents hold at least a first degree. This shows that emphasis is led on education and training. All the staff has also gone through specialized training with little of the respondent with years of experience between 1 to 3 years. This is in support of Vacca (2005) who says that adequate training will ensure that the right skills are put in place in other to increase the prosecution of Crime. Findings in this research also has respondents agreed that prosecution of Crime has increased because of forensic activities as supported by the work of Galves and Galves (2004) that purported that electronic trail exposes an outstanding probative digital fingerprint that can potentially be used to prove a criminal conduct in a court of law.

This research also reveals that respondents agreed that related laws like the Cyber Crime Act, 2015 and Evidence Act, 2011 (as amended) form basis for the acceptance of all evidences in both criminal and administrative proceedings. This is in relation to the suggestion by Van Rooyen (2004) that investigators must always execute their mandate within the ambit of the law and its limitations if any. This also align with the conclusions of Swanson, Chamelin and Territo (2003) and Joubert (2001) that maintains that evidence must be collected in accordance with the constitution and relevant laws. The conclusion is also supported by Shah (2002) who purported that investigators should always recognise the law and human rights. It is therefore established in this study that more prosecutions has been made between 2011 and 2017 which is as a result of the relevant laws enacted and amended.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Summary

This study has examined the effect of Digital forensic on Crime detection in Nigeria. Specifically, the study examined types of Digital forensic namely Computer forensic, Mobile forensic, and Network forensic and how they affect Crime detection. Consequently, Chapter one provide background to Digital forensic, it also addressed the statement of research problem, objective of the study, research questions, significance of the study, scope of the study, and definitions of operational terms.

Conceptual framework, theoretical framework and relevant literature were reviewed. The chapter extensively reviewed previous related studies, opinions, observation, ideas that shed light on the key concepts under consideration. The main issues discussed and reviewed revolved around Computer forensic, Mobile forensic, Network forensic, and Crime detection. Journals, published papers, conference proceedings and internet sources have been explored to extract relevant and current information about the major concepts earlier mentioned. Adequate effort was made to link the individual contribution of the researchers and academician in the field under review to the effect of digital forensic with emphasis on Computer forensic, Mobile forensic, and Network forensic as it relates to Crime detection.

The research work discussed the methodology used. It essentially examined the research design, the population and sample selection, data collection instruments, data analysis techniques and associated methodological issues that were encountered. The validity and reliability test as well as the justification of data analysis approach adopted were discussed. Cross tabulation were used to describe the data while multiple regression model was used

considering the relationship between the variables. Data for the study were gathered from forensic staff in 3 major law enforcement agencies. The instrument used to gather data was a well structured questionnaire using likert scale. The population for the study was limited and consequently, the whole of the 49 subjects were studied with questionnaires distributed, filled, returned, and analyzed.

Data presentation, data analysis, and discussion of findings were also discussed. Hypotheses were tested and results presented. The descriptive statistics involves representation of frequencies and percentages in the form of a cross tabulation. Multiple regression model was used to determine the relationship between the dependent and independents variables of the study. The result of research question one shows that Computer forensic has a significant effect on Crime detection. Findings show that in acquiring, analysing, examining, and reporting the occurrence of an investigation, proper forensic procedures and principles were used. The research also note and emphasized that the integrity of evidence are well protection and thereby increase the efficient of Computer forensic in Crime prosecution. So also, the research also revealed that Mobile forensic significantly affect Crime detection. Actors involved in the Crime, the action taken, and the state of interest of a Crime are ensured with adequate Mobile forensic procedures. Network forensic has significant affect of Crime detection as shown in this research. It was also noted that rate of prosecution has increased since the law enforcement agency started engaging forensic approaches to Crime investigation. Some scholars support the view of this research as regards to relevant laws that made digital forensic acceptable in a court of law. Such laws in Nigeria are Cyber Crime Act 2015, and the Evidence Act 2011 as amended.

5.2 Conclusion

The study shows that Digital forensic significantly affect Crime detection in Nigeria. Emphasis were led on three types of Digital forensic namely; Computer forensic, Mobile forensic, and Network forensic in relation to how they affect the detection and prevention of Crime. It was observed that Computer forensic has a significant effect on Crime detection and adequate attention should be paid to this as it has helped in the detection and prevention of crime according to the result of the data presented. By implicated, law enforcement need to be trained and equipped to adequately use Computer forensic tools. The same applied to Mobile and Network forensic as they both have significant effect on Crime detection in Nigeria. Though at infancy, the adoption of Digital forensic has improved the way investigation is done and digital evidence which the Evidence Act 2011 and Cyber Crime Act 2015 enhanced its acceptance in court of law is being used to resolve mostly unsolved crimes if traditional investigation methods were to be applied. Law enforcement in Nigeria therefore needs to intensify effort in making sure that Digital forensic break even so as to further strengthen the course of Crime Investigation.

5.3 Recommendations

Based on the findings and conclusion from the study, the following recommendations are made:

i. It was observed that Computer forensic has a significant effect on detection of Crime in Nigeria. In view of this, law enforcement agencies should continue to uphold the adoption of Computer forensic in both criminal and administrative investigation so as to further increase the rate of Crime detection, and prosecution.

ii. Mobile forensic has little significance on Crime detection in Nigeria due to the complexities and evolving nature of mobile technology. Based on this, more staff need to be employed and trained in this area to cope with the ever increasing crime rate as most criminals do have a level of mobile communications linkages.

iii. Cyber crime is at its increase, and cyber crime act as enacted in 2015 has provided basis for cyber prosecution in Nigeria. Network forensic which is significant to crime detection will help greatly in the detection and prosecution of such crimes. Adequate attention is to be paid to Network forensic because it will help law enforcement in breaking new grounds in cyber related crime investigation.

iv. Cyber Crime Act 2015 and the Evidence Act 2011 have helped in the acceptance of digital evidences in both criminal and civil cases. As such, more laws, policies, and act should be enacted to support and further strengthen digital forensics which seems to be at its infancy stage in Nigeria. This will increase its effectiveness in the detection and prevention of Crime in Nigeria.

5.4 Limitation of the Study

This study was faced with some limitations. The quality of data may be a limitation. This study made use of 49 respondents which happens to be the whole population. This sample is quite small for such a research of this magnitude. Also, accuracy of the data retrieved as response from the population could not be ascertain because it is difficult to measure whether the responses truly reflected their opinion bearing in mind the oath of secrecy and confidentiality. These limitations however did not affect the results of the study as they were overcome by careful administration of the research instrument and also instilling confidence in the respondents about the confidentiality of their responses.

REFERENCES

Agnew R. (1992): Foundation for a general strain theory of crime and delinquency. Criminology. 1992;30:47–87.

Agnew R.(1997): Stability and change in crime over the life course: A strain theory explanation. In: Thornberry TP, editor. Developmental Theories of Crime and Delinquency, Advances in Criminological Theory. Vol. 7. Transaction; New Brunswick, NJ: 1997. pp. 101–132.

Agnew R. (2006): Pressured into Crime: An overview of General Strain Theory. Roxbury Publishing; Los Angeles, CA: 2006.

Aljazeera (2005). Phone Dealers in al-Hariri Probe Net, URL, http://english.aljazeera.net/archive/2005/09/200841014558113928.html, (Accessed 1 July 2018).

Amanda, L. (2010). Teens and Mobile Phones 2010+ Pew Research Centre <http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP-Teens-and-Mobile-2010-with-topline.pdf>accessed 1July 2018.

Anderson, D. (2015). A Question of Trust – Report of the Investigatory Powers Review. *Independent Reviewer of Terrorism Legislation*. Retrieved on 1July 2018 from https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

Andrew, M. A (2009). Mobile phones Forensics <http:/www.martinandrew@martinsecurity.net http://www.martinsecurity.net > accessed on 1 July 2018.

Association of Chief Police Officers (2009). *ACPO e-crime strategy*. Retrieved on 1 July 2018 from http://itlaw.wikia.com/wiki/ACPO_e-Crime_Strategy.

Australian Institute of Criminology (2011). Definitions and general information. *Australian Government*. Retrieved on 1 July 2018 fromhttp://www.aic.gov.au/crime_types/cyber crime/definitions.html.

Ballin, H., & Ballin, M. F. H. (2012). *Anticipative criminal investigation - Rule of law Principles for counterterrorism*. The Hague, Netherlands: T.M.C. Asser Press.

Barran, M. L., and Jones, J. E. (2016). *Mixed Methods Research for Improved Scientific Study.* USA: Information Science Reference (IGI Global).

Beccaria C. (1963): First English edition 1767. On Crimes and Punishment, translated by H. Paolucci. Indianapolis, IN: Bobbs-Merrill Educational, 1963.

Berghel, H. (2003). The discipline of Internet Forensics. *Communications of the ACM,* 46(8), 15-20.

Bermay, F. P., & Godlove, N. (2012). Understanding 21st century cybercrime from the

'common' victim'. *Criminal Justice Matters*, *89*(1), 4-5.

Bhattacharjee, Y. (2011). How a remote town in Romania has become cybercrime central. *Wired*. Retrieved on 1 July 2018 from http://www.wired.com/magazine/2011/01/ff_hackerville_romania/all/.

Bocij, ., & McFarlane, L. (2003). *Cyberstalking: The technology of hate. The Police Journal*, *76*, 204-221.

Brenner, S. W. (2008). *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press.

Broadhurst, R. Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber Crime: An Analysis of the Nature of Croups engaged in Cyber Crime. *InternationalJournal of Cyber Criminology*, *8*(1), 1-20. Retrieved on 1 July 2018 fromhttp://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf.

Brown, C. S. D. (2015). Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities. In J. L. Richet (Ed.), *CybersecurityPolicies and Strategies for Cyberwarfare Prevention* (pp. 166-203). Hershey, PA: IGI Global.

Bryman, A. (2004). *Social Research Methods.* Oxford: Oxford University Press.

Bryant, R. (2008). *Investigating digital crime.* London: John Wiley & Sons Ltd.

Bushway S, Piquero A, Broidy LM, Cauffman E, Mazerolle P.(2001): An empirical framework for studying desistance as a process. Criminology. 2001;39:491–516.

Byrd, M. (2004). *Duty description to the crime scene investigator*. Miami: Miami Dade Police Department.

Canalys (2007). *Smart mobile device shipments hit 118 million in 2007*, up 53% on 2006, URL, http://www.canalys.com/pr/2008/r2008021.htm, (Accessed 1 July 2018).

Cardwell, K., Clinton, T., Cohen, T., Collins, E., Cornell, J., Cross, M., Depew, L., Ehuan, A., Gregg, M., Jean, B.R., O'Shea, K., Reis, K., Reyes, A., Schuler, K., Schneider, S., Schroader, A., Varsalone, J., Wiles, J. & Wright, C. (2007). *The best damn cybercrime and digital forensics book period*. Burlington: Syngress Publishing.

Casey, E. (2004). *Digital evidence and computer crime: Forensic Science, computers and the internet.* 2nd edition. Florida: Academic Press.

Chen, A. (2015). The Agency. *The New York Times Magazine*. Retrieved 1 July 2018 from http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.*Cybercrime*. Report prepared for the Open-Ended Intergovernmental Expert Group onCyber crime. New York: United Nations. Retrieved on 1 July 2018 fromhttps://www.unodc.org/documents/organized-

Chisum, W.J. & Turvey, B. (2000). Evidence dynamic: Locard's exchange principle. Crime

Reconstruction. *Journal of Behavioural Profiling*, 1, January:1-15.

Clapper, J. R. (2015). Worldwide Threat Assessment of the US Intelligence Community. Statement for the record by James R. Clapper, Director of National Intelligence, for the *Senate Armed Services Committee*. Retrieved 1July 2018 from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

Clarke R.V.G.(1987): Rational Choice Theory and Prison Psychology, in BJ McGurk D. Thorton and M. Williams eds Applying Psychology to Imprisonment: Theory and Practice. London: HMSO, 1987.

Cornish D.B., Clarke R.V.G.(1986): The Reasoning Criminal. New York: Springer Verlag, 1986.

Craiger, J.P. & Shenoi, S. (2007). *Advances in digital forensics III.* Boston: Springer.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. (3rd Ed.). Thousand Okas, CA: Sage.

CrowdStrike (2015). 2014 Global Threat Intel Report. *CrowdStrike Threat Intel*.

Cross, M. (2008). *Scene of the cybercrime.* 2nd edition. Arlington: Syngress Publishing.

Curran, K., Robinson, A., Peacocke, S. and Cassidy, S. (2010). Mobile Phone Forensic Analysis, International Journal of Digital Crime and Forensics, Vol 2, No 2, pp, April-May 2010, ISSN: 1941-6210 IGI Pub <eprintsectionulster.ac.uk/20680/2/IJCDF10.pdf> accessed 1 July 2018.

Curtis, K. (2011). A mobile phone records a fatal stabbing, becomes key evidence at a murder trial < http://www.tampabay.com/news/Courts/criminal/a-cell-phone-records-a-fatal-stabbing-becomes-key-evidence-at-a-murder/1150310>accessed 1 July 2018.

Cyber Crime Act, 2015.

Dambazau, A.B. (2007) *Criminology and Criminal Justice* 2nd Edition. Ibadan: University Press.

Davies, M. (1999). Failing to Deliver on Cyber Crime. *Birmingham Post.*

Dee, M. (2012). Getting back to the Fourth Amendment: Warrantless cell phone searches. *New York Law School Law Review*, *56*, 1129-1163. Retrieved on 26thFebruary 2015 from http://www.nylslawreview.com/wp-content/uploads/sites/16/2012/02/Dee-note.pdf.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla & D. F. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 239–288). Santa Monica:RAND.

Det, M. C. (2011). Cellular Phone Evidence; Data Extraction and Documentation, Developing Process For The Examination Of Cellular Phone Evidence"<http://ccf.cs.uml.edu/forensicspapers/Cellular%20Phone%20Evidence%20Data%20Extraction%20and%20Documentation.pdf>accessed 1 July 2018.

Doran, P. (2008). 2008- the year of mobile customers, URL, http://www.themda.org/documents/PressReleases/General/_MDA_future_of_mobile_press_release_Nov07.pdf (Accessed 1 July 2018).

D'Ovidio, R., & Doyle J. (2003). A study on Cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin*, *72*(3), 10-17.

Dubord, P. (2008). Investigating Cybercrime. In J. J. Barbara (Ed.), *Handbook of Digitaland Multimedia Forensic Evidence* (pp. 77-89). Totowa, NJ: Humana Press Inc.

Emmanuel, S. P., Joshi, R. C., and Rajdeep, N. (2010). A Generic Framework for Network Forensics. *International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 11*.

Endgame (2015). Turn the map around to prevent damage and loss from cyber attack. *Endgame White Paper*. Retrieved on 1 July 2018 from http://pages.endgame.com/WC2015

Farrington, D. P.(1992): Criminal career research in the United Kingdom. British Journal of Criminology. 1992;32:521–536.

Felson, M., Clarke, R.V.G.(1998): Opportunity Makes the Thief. London: Home Office, 1998.

FireEye Labs (2015). APT30 and the mechanics of a long-running cyber espionage operation. *FireEye Threat Intelligence Special Report*. Retrieved 1 July 2018 from https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf.

Fisher, B.A.J. (2004). *Techniques of crime scene investigation.* 7th edition. Washington D.C: CRC.

Frolova, I. (2011). Real punishment for virtual criminals. *Voice of Russia*.

Gallagher, S.R & Aro, E.P. (2005). *Evolving standards for discovery in the electronic age.* Colorado: Hogan & Hartson. From:http://www.abanet.org/buslaw/newsletter/0036/materials/pp8.pdf(accessed 1 July 2018).

Galves, F. & Galves, C. (2004). Ensuring the admissibility of electronic forensic evidence and enhancing its probative value at trial. *Criminal Justice Magazine,* 19(1):3. From: http ://www.abanet.org/crimjust/cjmag/home.html (accessed 1 July 2008).

Gary, P. (2001). A Road Map for Digital Forensic Research Technical Report DTR-T0010-

01 DFRWS. Report from the First Digital Forensic Research Workshop (DFRWS); Brian Carrier,'Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers' Winter 2003, Volume 1, Issue 4 International Journal of Digital evidence <digital4nzicsectioncom/.../Defining%20Digital%20Forensic%20Examination>accessed 1 July 2018.

Geist, M. (2003). Cyber Law 2.0. *Boston College Law Review, 44*(2), 359-396.

Gilbert, J. N. (2004). *Criminal Investigations*, 6th edition. Upper Saddle River, New Jersey:

Girodo, M., Deck, T., & Morrison, M. (2002). Dissociative-type identity disturbances in undercover agents: Socio-cognitive factors behind false-identity appearances and reenactments. *Social Behavior and Personality, 30,* 631-644.

Goodno, N. H. (2007). Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws. *Missouri Law Review, 72,* 125-196.

Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology, 10*(2), 139-223.

Golden, T.W., Skalak, S.L. & Clayton, M.M. (2006). *A guide to forensic accounting investigation.* New Jersey: John Wiley & Sons.

Gordon S., & Ford, R. (2006). On the Definition and Classification of Cyber crime. *Journal of Computer Virology, 2*(1), 13-20.

Gottfredson, M., Hirschi, T. A.(1990): General Theory of Crime. Stanford University Press; Stanford, CA: 1990.

Grace T., & Mell, P. (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology. NIST Special Publication, No 800-145. National Institute of Standards and Technology: United States Department of Commerce. Retrieved on 1 July 2018 from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Gunnison, E., Mazerolle, P.(2007): Desistance from serious and not so serious crime: A comparison of psychological risk factors. Criminal Justice Studies. 2007;20:231–253.

Hammond, M., & Wellington, J. J. (2013). *Research methods: The key concepts*. London: Routledge.

Healy, L. (2008). Increasing the Likelihood of admissible electronic evidence: Digital log Handling excellence and a forensically aware corporate culture Available (online): http://www.emich.edu/ia/pdf/phdresearch/Increasing%20the%20Likelihood%20of%20Admissible%20Electronic%20Evidence,%20Larry%20H ealy%20COT%20704.pdf. Accessed on 1 July, 2018.

Herrera-Flanigan, J. R., & Ghosh, S. (2010). Criminal Regulations. In S. Ghosh & E.

Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis*, (pp. 265-308). Berlin: Springer.

Hoog, A. (2014). "Chapter 3. Cellebrite UFED-2014". Via Forensics Accessed 1 July, 2018.

Holmes, S. (2006). *An overview of criminal investigation.* New York: Clarkson N. Potter. From: http://www.apsu.edu/oconnort/3220/3220lect01.htm (accessed 1 July 2018).

Holt, T. J. (2012). Exploring the Intersections of Technology, Crime, and Terror. *Terrorism and Political Violence*, *24*(2), 337-354.

Horswell, J. (2004). Crime scene investigation and third party quality systems accreditation: Australia's experience. In J. Horswell (Ed.), *The Practice of Crime SceneInvestigation*. Boca Raton: CRC Press.

Horswell, J. (2004). *The practice of crime scene investigation.* Washington D.C.: CRC.

Hrycko, O. (2007). *Electronic discovery in Canada: Best practices and guidelines*. Toronto: CCH Canadian.

Hughes, J. (2003). The Internet and the Persistence of Law. *Boston College Law Review*, *44*(2), 359-396.

Jaya N. (2010). 'Face of the 'happy slap' killer: Sadist who murdered girlfriend's toddler jailed for 26 years Mail Online (London, 3 December 2010)http://www.dailymail.co.uk/news/article-1335042/Darren-Newton-guilty-Charlie-Hunt-murder-happy-slap-attack-filmed > accessed 1 July 2018.

Joubert, C. (2001). *Applied law for police officials.* 2nd edition. Cape Town: Juta Legal and Academic Publishers.

Karagiozis, M.F. & Sgaglio, R. (2005). *Forensic investigation handbook: An introduction to the collection, preservation, analysis and presentation of evidence*. Illionis: CharlesC Thomas Publisher.

Katie, B. and Eric, L. (2016). U.SECTION Says It Has Unlocked iPhone Without Apple *The New York Times*http://www.nytimesectioncom/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0 accessed 20th July 2016 Kevin Johnson, Jon Swartz and Marco della Cava, USA TODAY 1:51 pm EDT March 29 2016 http://www.usatoday.com/story/news/nation/2016/03/28/apple-justice-department farook/82354040/ Accessed 1 July 2018.

Kaspersky Lab (2015). Carbanak APT: The Great Bank Robbery. *Securelist*. Retrieved on 1 July 2018, from *Katz v United States*, 839 US 347.

Kaye, B. H. (1995). *Science and the Detective – Selected Reading in Forensic Science*. New York: VCH Verlagsgesellschaft.

Kazemian, L.(2007): Desistance from crime: Theoretical, empirical, methodological, and policy considerations. Journal of Contemporary Criminal Justice. 2007;23:5–27.

Keane, A. (2000). *The modern law of evidence.* 5th edition. London: Butterworths.

Keonwoo, K. (2007). Data Acquisition from Mobile phone using Logical Approach. World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering<waset.org/.../data-acquisition-from-cell-phone-using-logical-approach>accessed 1 July 2018.

Kovacich, G.L. & Boni, W.C. (2000). *High-technology-crime investigator's handbook: Working in the global information environment*. Burlington: Butterworth-Heinemann Publications.

Kozushko, H. (2003). *Digital evidence graduate seminar.* New Mexico Tech-Computer Science Department. From: http://www.infosyssec.org/infosyssec/.../forensicevidence1.html (accessed 1 July 2018).

Kshetri, N. (2010). *Global Cybercrime Industry: Economic, institutional and strategic perspectives*. Berlin Heidelberg: Springer Science & Business Media.

Lambrechts, D. (2001). Forensic investigation. Pollex. *Servamus*, 94(10):93.

Lange, M.C.S. & Nimsger, K.M. (2004). *Electronic evidence and discovery: What every lawyer should know*. Chicago: ABA Publishing.

Laub, J.H., Sampson, R.J.(2001): Understanding desistance from crime. In: Tonry M, editor. Crime and Justice. Vol. 28. University of Chicago Press; Chicago: 2001. pp. 1–69.

Lee, H.C., Palmbach, T. and Miller, M.T. (2003). *Crime scene handbook.* London: Academic.

Leibolt, G. (2010). The Complex World of Corporate Cyber Forensics Investigations. In J. Bayuk (Ed.), *CyberForensics* (pp. 7-27). New York: Springer Science Business Media.

Lidsky, L. B., & Cotter, T. (2007). Authorship, Audiences, and Anonymous Speech. *NotreDame Law Review*, *82*, 1537-1604.

Loeber, R., LeBlanc, M.(1990): Toward a developmental criminology. In: Tonry M, Morris N, editors. Crime and Justice. University of Chicago Press; Chicago: 1990. pp. 375–473.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60

Manfrediz, A. (2008). *IDC Press Release. IDC Finds More of the World's Population Connecting to the Internet in New Ways and Embracing* Web 2.0 Activities, URL, http://www.idc.com/getdoc.jsp?containerId=prUS21303808, (Accessed 1 July 2018).

Marud, M. (2004). *Argus*, 27 May: 28

Maruna, S.(2001): Making good, How ex-convicts reform and rebuild their lives. American Psychological Association; Washington, DC: 2001.

McQuade III, S. C. (2006). *Understanding and Managing Cybercrime*. New York: Pearson Education, Inc.

Mills, E. (2012). Cybercrime moves to the cloud. *CNET Australia*. Retrieved on 1 July 2018 from http://www.cnet.com/news/cyber crime-moves-to-the-cloud/.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005).The Internet and family and acquaintance sexual abuse. *Child Maltreat*, *10*, 49-60.

Mohay, G.M., Anderson, A., Collie, B., De Vel., O. & McKemmish, R.D. (2003). *Computer and intrusion forensics.* Boston: Artech House.

Mutnick, K. D., & Simon, L. W. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley Publishing John Wiley & Sons, Inc

National Institute of Justice. (2002). Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyberterrorism, Princeton NJ.

Nelly, L. (2016). Beware of Imitators. Al-Qa'ida Through the Lens of its Confidential'< https://www.ctc.usma.edu/.../beware-of-imitators-al-qaida >Accessed 1July 2018.

Nigerian Evidence Act, (2011).

Nuth, M. S. (2008). Crime and technology – Challenges or solutions? Taking advantage of new technologies: For and against crime. *Computer Law & Security Report*, *24*, 437– 446.

Nwana, O. C. (2005). *Introduction to Educational Research.* Ibadan: Heinemann Educational Books (Nig) Plc.

O'Hara, C. (1962). *Modern criminal investigation*. 5th edition. New York: Funk & Wagnalls.

O'Shea, T. M. and Darnell, J. (2011). Obtaining and admitting electronic evidence; Admissibility of Forensic Mobile phone Evidence. United States Attorneys' Bulletin42 <www.justice.gov/sites/default/files/usao/legacy/2011/11/...30/usab5906.pdf >accessed 1 July 2018.

Okunola, R. (2002). *Crime in Society* cited in Current Perspectives in Sociology.

Omeleze, S., and Venter, H. S.(2015). Towards a Model for Acquiring Digital Evidence using Mobile phones.

Onyshikiv, Y., & Bondarev, A. (2012). Ukraine thrives as cyber crime haven. *Kyiv*

Post. Retrieved on 1 July 2018 from http://smart-payments.info/eng/publication-one/124.html.

Osborne, C. (2012). For investigators, a better way to extract data from mobile phones. SmartPlanet.com.<http://www.zdnet.com/article/for-investigators-a-better-way-to-extract-data-from-mobile-devices> accessed 1 July 2018.

Palmer, G. L. (2001). A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS).

Palmiotto, M.J. (1998). *Criminal investigations.* 2nd edition. Wichita: Austin & Winfield.

Peisert, S., Bishop, M., Marzullo, K. (2008). Computer forensics in forensis. ACM SIGOPS Operating Systems Review 42(3)

Perry, W. G. (2009). Information Warfare: Assuring Digital Intelligence Collection. The Joint Special Operations University (JSOU) Press, Hurlburt Field, Florida, 2009. Available: https://ntrl.ntis.gov/NTRL/dashboard/searchResults/titleDetail/ADA514505.xhtml (Accessed 1 July 2018).

Piquero, A., Farrington, D., Blumstein, A.(2003). The criminal career paradigm. In: Tonry M, editor. Crime and Justice: A review of the research. Vol. 30. University of Chicago Press; Chicago: 2003. pp. 359–506.

Pocar, F. (2004). Defining Cyber-Crimes in International Legislation. *European Journal On Criminal Policy and Research*, *10*, 27–37.

Post, J. M., Ruby, K. G., & Shaw, E. D. (2000). From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *Terrorism and Political Violence*, *12*, 97– 122.

Pollitt, M. M. (2001). Report on digital evidence: Paper delivered at the 13th International Criminal Police Organization forensic science symposium. From: http://www.interpol.int/public/Forensic/IFSS/meeting13/Reviews/Digital.pdf (accessed 1 July 2018).

Pollitt, M. M. (2007). An ad hoc review of digital forensic models, In Systematic Approaches to Digital Forensic Engineering, 2007, pages 43{54. University of Central Florida, USA, IEEE, April 10- 12, 2007.

Ponemon Institute (2015). 2015 cost of data breach study: Global analysis. *Ponemon Institute Research Report*. Retrieved on 1 July 2018 fromhttp://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF

Ranum, M. (2012). "Is Network Intrusion Detection Software Being Used Correctly?" (Available at http://www.securitvmanaement.com/li brq/00556.html).

Raymond, T (2006). The Future for Forensic Scientists. *Australian Journal of Forensic Sciences*, *38*(1), 3-21.

Raysman, R. and Brown, P. (1984). *Computer law: Drafting and negotiating forms and agreements*. New York: Law Journal Press.

Rick, A., Sam, B. and Wayne, J. (2013). Guidelines on Mobile phone Forensics. Recommendations of theNational Institute of Standards and Technology. NIST Special Publication 800-101 Revision 1< http://nvlpubsectionnist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>accessed 1 July 2018.

Robertson, J., Riley, M., Strohm, C., & Chan, M. (2014). The year of hacking dangerously - 7 scary cyberattacks. *Bloomberg*. Retrieved on 1 July 2018 from http://www.bloomberg.com/slideshow/2014-12-10/the-year-of-hacking-dangerously.html?#slide1.

Ruibin, G. Garrtner, M. (2005). Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework. Vol. 4(1) Available (Online): http://www.utica.edu/academic/institutes/ecii/publications/articles/B4A6A102-A93D-85B1-95C575D5E35F3764.pdf Accessed 1July 2018.

Sam B. (2009). Mobile phone and GPS Forensic Tool Classification System" http://www.mobileforensicsworld.org/2009/presentations/MFW2009_BROTHERS_CellPhonean GPS ForensicTool Classification System.pdf <accessed> 1 July 2018.

Samanthi, W. and Sunesh, H. (2016). Use of Computer Forensics and its Implication. Retrieved on 1 July 2018 from https://www.researchgate.net/publication/307107635

Satish, B., Rohit, T. and Heather M. (2016). Practical Mobile Forensics https://www.amazon.com/Practical-Mobile-Forensics-Satish-Bommi< accessed> 1 July 2018.

Savona, E. U., and Mignone, M. (2004). The Fox and The Hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research*, *10*, 2-26.

Scientific Working Group on Digital Evidence (SWGDE) (2000). Proposed Standards for the Exchange of Digital Evidence. *Forensic Science Communications*, *2*(2).Retrieved on 1 July 2018 from http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/.

Sean C. S. (2008). Mobile phone Forensics Case File Integrity Verification' Degree of Master of Science, PurdueUniversity May 2008 < framework.zend.com/issues/secure/attachment/11259/Thesis-broken.pdf>Accessed 1 July 2018.

Selamat, R.S., Sahib, S., Hafeizah, N., Yosof, R., and Abdollar, M.F., (2013). A Forensic

Traceability Index in Digital Forensic Investigation. Journal of Information Security, Vol.4.19-32

Shafritz, R. (2001). A Survey of Cyberstalking Legislation. *UWLA Law Review, 32*, 223-338.

Shah, G. (2002). *Investigation of crime and criminals.* New Delhi: Anmol Publications.

Shira, A., Scheindlin, S.A. and Rabkin, J. (2000). Electronic discovery in federal civil litigation: Is rule 34 up to the task? *B. C. L. Rev*, 41(2) March:327-338.From: http://www.bc.edu/bc_org/avp/law/lwsch/journals/bclawr/412/03FMS.html (accessed 1 July 2018).

Silvernail, S.J. (1997). Electronic Evidence: Discovery in the Computer Age. *The Alabama Lawyer,* 58, May:176-177.

Simms, B.W. and Petersen, E.R. (1991). An information processing model of a police organization. *Management Science,* 37(2), February:216.

Smith, R. G. (2004). Impediments to the Successful Investigation of Transnational High Tech Crime. *Trends and Issues in Crime and Criminal Justice*, no. 285, Australian Institute of Criminology. Retrieved on 1 July 2018 from http://www.aic.gov.au/documents/0/7/6/%7B076B58BA-37AE-4673-93FB-9C3150D93D0C%7Dtandi285.pdf.

Snyder, F. (2001). Sites of criminality and sites of governance. *Social & Legal Studies*, *10*, 251–256.

Spitzberg, B. H., and Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4*(1), 71-92.

Stanley, S., and Horswell, J. (2004). The education and training of crime scene investigators: an Australian Perspective. In J Horswell (Ed.), *The Practice of Crime Scene Investigation*. Boca Raton: CRC Press.

Stephenson, P. (2000). *Investigating computer-related crime.* Florida: CRC Press.

Stippich, M.J. (2006). *Electronic evidence: Issues.* Wisconsin: Wisconsin Bar Association. From:https://www.wisbar.org/AM/TemplateRedirect.cfm?template=/CM/ContentDisplay.cfm&ContentID=61964 (accessed 1 July 2018).

Swanepoel, J. (2001). *Rights and powers of private investigation*: Paper delivered at the second world conference on modern criminal investigation, organised crime and human rights. Durban. 3-7 December 2001.

Swanson, C.R., Chamelin, N.C. & Territo, L. (2003). *Criminal investigation*. 8th edition. Boston: McCraw-Hill.

Taylor, C. (2003). *An introduction to metadata.* University of Queensland Library. From:

http://74.125.77.132/search?q=cache:1koOCagFsgJ:www.library.uq.edu.au/iad/ctmmeta4.html+metadata&cd=2&hl=en&ct=clnk (accessed 1 July 2018).

Tetzlaff-Bemiller, M. J. (2011). Undercover Online: An Extension of Traditional Policing in the United States. *International Journal of Cyber Criminology*, *5*, 813-824.

Uggen, C., Piliavin, I.(1998): Assymetrical causation and criminal desistance. Journal of Criminal Law and Criminology. 1998;88:1399–1422.

U.S. Department of Justice (2010). A Review of the FBI's Investigations of Certain Domestic Advocacy Groups. *Office of the Inspector General*. Retrieved on 1 July 2018 from http://www.justice.gov/oig/special/s1009r.pdf.

United Nations Office on Drugs and Crime (2013). *Comprehensive Study on Drugs and Crime.*

Vacca, J. (2005). *Computer forensics – Computer crime scene investigation.* 2nd edition. Hingham: Charles River Media.

Vadackumchery, J. (2003). *Crime law and police science.* New Delhi: Concept Publishing Company.

Van Rooyen, H.J.N. (2004). *The A-Z of investigation: A practical guide for private and corporate investigators.* Pretoria: Crime Solve.

Van der Westhuizen, J. (1996). *Forensic criminalistics.* 2nd edition. Johannesburg: Heinemann.

Volonino, L. (2003). Electronic evidence and computer forensics. *Communications of the Association for Information Systems*, 12(27): From:http://138.92.8.227/Volonino-CAIS-Journal.pdf. (accessed 1 July 2018).

Walden, I. (2005). Crime and Security in Cyberspace. *Cambridge Review of International Affairs*, *18*(1), 51-68.

Wall, D. S. (2001). Cybercrimes and Criminal Justice. *Criminal Justice Matters*, *46*(1), 36-37.

Wall, D., and Williams, M. (2001). Policing diversity in the digital age: Maintaining order in virtual communities. *Journal of Criminology and Criminal Justice*, *7*, 391–415.

Waltz, E. (1998). *Information Warfare*. Norwood: Artech House.

Ward, R.H. (1975). *Introduction to criminal investigation.* Philippines: Addison-Wesley Publishing Company.

Westtek (2008). *ClearVue Suite*, URL http://www.westtek.com/smartphone/, (Accessed 1 July 2018).

Weston, P.B., Lushbaugh, C. and Wells, K.M. (2000). *Criminal investigation: Basic perspectives*. New Jersey: Prentice Hall. White, P. C. (2004). *Crime Scene to Court: The Essentials of Forensic Science*, 2nd edition.

Whitfield, L. (2012). "Forensic 4cast Awards 2012 – Results". Accessed 1 July 2018.

Wolf, J. B. (2000). War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money. *American Journal of Criminal Law*, *25*, 95-117.

Yar, M. (2005). The novelty of `cyber crime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*, 407–427.

Zatyko, K. (2007). Commentary: Defining Digital Forensics. Retrieved 1 July 2018, from: http://www.forensicmag.com/node/128

Zatyko, K., & Bay, J. (2011). The digital forensics cyber exchange principle. *Forensic Magazine*. Retrieved on 1 July 2018 from http://www.forensicmag.com/articles/2011/12/digital-forensics-cyber-exchange-principle.

Zavrsnik, A. (2010). Towards an Overregulated Cyberspace. *Masaryk University Journal of Law & Technology*, *4*(2), 173-190.

APPENDIX I

QUESTIONNAIRE

NASARAWA STATE UNIVERSITY, KEFFI
INSTITUTE OF GOVERNANCE AND DEVELOPMENT STUDIES

My name is Ajayi Oluwashina Joseph. I am currently conducting a research on the topic titled "Effect of Digital Forensic Techniques on Crime Detection in Nigeria". I will be pleased if you can help in responding to the questions below. Your responses should be relative to the crimes from 2011 to 2017. Your answers to these questions will be very helpful to this research. I assure you that the result will be used for academic purpose only and your personal information shall be treated with outmost confidentiality.

Thank you for your time and cooperation.

Please answer all questions. Select only one option that is best applicable.

Section A: General Information (Tick as appropriate)

1. Name of your Agency: EFCC [ ] ICPC [ ] NPF [ ]
2. Years of Experience in Digital Forensics (in years): 1-3 [ ] 4-7 [ ] More than 7 [ ]
3. Level of Education: Nation Diploma [ ] Graduate (Bachelor's/HND) [ ] Postgraduate (PGD/MSc/PhD) [ ]

On Section B to D below, please rate the statement on a scale of 1-5, where 5 = "Strongly Agree(SA)", 2 = "Agree (A)", 3 = "Undecided(U)", 4 = "Disagree(D)", and 5 = "Strongly Disagree(SD)"

Section B: Computer Forensic and Crime Detection

No	ITEMS	SA 5	A 4	U 3	D 2	SD 1
B1	I follow all general Computer Forensic procedure and principles while identifying and collecting digital evidence					
B2	I ensure action taken do not change evidence and its integrity are kept intact					
B3	I ensure all evidences collected are analyzed without modifying them					
B4	All activities related to seizure, access, storage or transfer of evidence are fully documented, preserved and available for review					
B5	I ensure that legally justifiable methods and techniques are used to derive useful information that address the crime committed					
SECTION C: Mobile Forensics and Crime Detection						
No	**ITEMS**	**SA 5**	**A 4**	**U 3**	**D 2**	**SD 1**
C1	I ensure that adequate measures are taken to protect the volatility nature of phone evidence					
C2	In Identifying actors, actions, and state of interest of a crime, I					

	ensure that standard procedures are taken					
C3	I ensure I do a proper anti-forensic check on Mobile devices while collecting and analysis evidence					
C4	I ensure a proper link analysis is done at the analysis phase to determine the extent of Crime and to validate the purpose of the Investigation					
	SECTION D: Network Forensic and Crime Detection					
No	**ITEMS**	**SA 5**	**A 4**	**U 3**	**D 2**	**SD 1**
D1	I ensure that evidences are collected through Network Packets, firewall logs, IDS logs, system logs, routers log and audit logs depending on the nature of crime					
D2	I pay adequate attention to anti-forensics techniques (Data hiding, IP hiding, Data Destruction etc.) while acquiring evidence					
D3	I ensure that evidences are validated in every step taken in analysis					
D4	To protect the integrity of evidence, I ensure that all deleted files from all sources are recovered for the Investigation					
	SECTION E: Crime Detection	**SA 5**	**A 4**	**U 3**	**D 2**	**SD 1**
E1	Computer Forensic has helped in detecting more crime than the traditional investigation methods based on my experience.					
E2	More breakthrough has been recorded in Crime detection with Mobile Forensic.					
E3	Network Forensic has helped greatly in resolving the anonymous nature of Network attack which usually poses challenge in Crime Detection.					
E4	Prosecution of crime has increased because of forensic activities.					
E5	The Cyber Crime Act, 2015 and Evidence Act 2011 have form basis for the acceptance of all our evidences in criminal and administrative proceedings.					

APPENDIX II

SUMMARIZED RESPONSES FROM THE QUESTIONNAIRE

Section B: Computer Forensic and Crime Detection – Responses from Questionnaires based on 5 points Likert Scale (SA -5, A -4, U -3, D- 2, SD - 1)						
Respondent	**B1**: I follow all general Computer Forensic procedure and principles while identifying and collecting digital evidence	**B2:** I ensure action taken do not change evidence and its integrity are kept intact	**B3:** I ensure all evidences collected are analyzed without modifying them	**B4:** All activities related to seizure, access, storage or transfer of evidence are fully documented, preserved and available for review	**B5:** I ensure that legally justifiable methods and techniques are used to derive useful information that address the crime committed	**Total**
1	5	5	5	5	5	**25**
2	4	4	4	3	2	**17**
3	5	5	5	5	5	**25**
4	4	4	4	4	4	**20**
5	5	5	5	5	5	**25**
6	5	4	5	4	5	**23**
7	5	4	5	4	5	**23**
8	5	4	5	4	5	**23**
9	5	3	5	4	5	**22**
10	5	2	5	4	5	**21**
11	5	2	5	3	5	**20**
12	5	2	5	2	5	**19**
13	5	1	3	2	5	**16**
14	5	5	3	2	5	**20**
15	4	5	4	1	5	**19**
16	4	5	4	5	5	**23**
17	4	5	4	5	4	**22**

18	4	5	4	5	4	**22**
19	3	5	4	5	4	**21**
20	3	5	4	5	4	**21**
21	2	5	2	5	1	**15**
22	2	5	1	5	2	**15**
23	1	5	1	5	3	**15**
24	5	5	5	5	5	**25**
25	4	4	4	3	2	**17**
26	5	5	5	5	5	**25**
27	4	4	4	4	4	**20**
28	5	3	5	4	5	**22**
29	5	2	5	4	5	**21**
30	5	2	5	3	5	**20**
31	5	2	5	2	5	**19**
32	5	1	3	2	5	**16**
33	5	5	3	2	5	**20**
34	4	5	4	1	5	**19**
35	4	5	4	5	5	**23**
36	4	5	4	5	4	**22**
37	4	5	4	5	4	**22**
38	5	5	5	5	5	**25**
39	4	4	4	3	2	**17**
40	5	5	5	5	5	**25**
41	4	4	4	4	4	**20**
42	5	5	5	5	5	**25**
43	5	4	5	4	5	**23**
44	5	4	5	4	5	**23**
45	5	4	5	4	5	**23**

46	5	5	5	5	5	**25**
47	4	4	4	4	4	**20**
48	4	4	4	4	4	**20**
49	5	5	5	5	5	**25**

Section C: Mobile Forensic and Crime Detection – Responses from Questionnaires based on 5 points Likert Scale (SA -5, A -4, U -3, D- 2, SD - 1)					
Respondents	**C1**: I ensure that adequate measures are taken to protect the volatility nature of phone evidence	**C2:** In Identifying actors, actions, and state of interest of a crime, I ensure that standard procedures are taken	**C3:** I ensure I do a proper anti-forensic check on Mobile devices while collecting and analysis evidence	**C4:** I ensure a proper link analysis is done at the analysis phase to determine the extent of Crime and to validate the purpose of the Investigation	**Total**
1	5	5	5	5	**20**
2	2	2	1	5	**10**
3	5	5	3	3	**16**
4	3	2	2	2	**9**
5	5	5	5	5	**20**
6	5	5	5	5	**20**
7	4	4	4	3	**15**
8	5	5	5	5	**20**
9	4	4	4	4	**16**
10	5	5	5	5	**20**
11	3	3	2	2	**10**
12	5	5	5	5	**20**
13	4	4	2	1	**11**
14	5	5	5	5	**20**
15	4	4	1	2	**11**
16	4	5	4	5	**18**

17	4	5	4	5	**18**
18	4	5	4	5	**18**
19	3	5	4	5	**17**
20	3	5	4	5	**17**
21	2	5	2	5	**14**
22	2	5	1	5	**13**
23	1	5	1	5	**12**
24	5	5	5	5	**20**
25	2	2	1	5	**10**
26	5	5	3	3	**16**
27	3	2	2	2	**9**
28	4	4	4	4	**16**
29	5	5	5	5	**20**
30	3	3	2	2	**10**
31	5	5	5	5	**20**
32	4	4	2	1	**11**
33	5	5	5	5	**20**
34	4	4	1	2	**11**
35	4	5	4	5	**18**
36	4	5	4	5	**18**
37	4	5	4	5	**18**
38	5	5	5	5	**20**
39	2	2	1	5	**10**
40	5	5	3	3	**16**
41	3	2	2	2	**9**
42	5	5	5	5	**20**
43	5	5	5	5	**20**
44	4	4	4	3	**15**

45	5	5	5	5	**20**
46	5	5	3	3	**16**
47	3	2	2	2	**9**
48	3	2	2	2	**9**
49	5	5	5	5	**20**

Section D: Network Forensic and Crime Detection – Responses from Questionnaires based on 5 points Likert Scale (SA -5, A -4, U -3, D- 2, SD - 1)					
Respondents	**D1:** I ensure that evidences are collected through Network Packets, firewall logs, IDS logs, system logs, routers log and audit logs depending on the nature of crime	**D2:** I pay adequate attention to anti-forensics techniques (Data hiding, IP hiding, Data Destruction etc.) while acquiring evidence	**D3**: I ensure that evidences are validated in every step taken in analysis	**D4**: To protect the integrity of evidence, I ensure that all deleted files from all sources are recovered for the Investigation	**Total**
1	4	4	4	4	**16**
2	5	5	5	5	**20**
3	4	4	4	4	**16**
4	1	5	5	5	**16**
5	5	5	4	4	**18**
6	5	5	5	5	**20**
7	2	2	2	1	**7**
8	5	5	5	3	**18**
9	4	3	2	2	**11**
10	5	5	5	5	**20**
11	1	3	3	2	**9**
12	5	5	5	5	**20**
13	1	4	4	2	**11**
14	5	5	5	5	**20**

15	3	4	4	1	**12**
16	5	4	5	4	**18**
17	4	4	5	4	**17**
18	4	4	5	4	**17**
19	4	3	5	4	**16**
20	4	3	5	4	**16**
21	1	2	5	2	**10**
22	2	2	5	1	**10**
23	3	1	5	1	**10**
24	4	4	4	4	**16**
25	5	5	5	5	**20**
26	4	4	4	4	**16**
27	1	5	5	5	**16**
28	4	3	2	2	**11**
29	5	5	5	5	**20**
30	1	3	3	2	**9**
31	5	5	5	5	**20**
32	1	4	4	2	**11**
33	5	5	5	5	**20**
34	3	4	4	1	**12**
35	5	4	5	4	**18**
36	4	4	5	4	**17**
37	4	4	5	4	**17**
38	4	4	4	4	**16**
39	5	5	5	5	**20**
40	4	4	4	4	**16**
41	1	5	5	5	**16**
42	5	5	4	4	**18**

43	5	5	5	5	**20**
44	2	2	2	1	**7**
45	5	5	5	3	**18**
46	4	4	4	4	**16**
47	1	5	5	5	**16**
48	1	5	5	5	**16**
49	5	5	4	4	**18**

Section E: Crime Detection – Responses from Questionnaires based on 5 points Likert Scale (SA -5, A -4, U -3, D- 2, SD - 1)						
Respondents	**E1:** Computer Forensic has helped in detecting more crime than the traditional investigation methods based on my experience.	**E2:** More breakthrough has been recorded in Crime detection with Mobile Forensic.	**E3:** Network Forensic has helped greatly in resolving the anonymous nature of Network attack which usually poses challenge in Crime Detection.	**E4:** Prosecution of crime has increased because of forensic activities.	**E5:** The Cyber Crime Act, 2015 and Evidence Act 2011 have form basis for the acceptance of all our evidences in criminal and administrative proceedings.	**Total**
1	3	3	2	2	1	**11**
2	5	5	5	5	5	**25**
3	4	4	2	1	1	**12**
4	5	5	5	5	5	**25**
5	4	4	1	2	3	**14**
6	5	4	4	4	4	**21**
7	5	5	5	5	5	**25**
8	3	4	4	4	4	**19**
9	2	1	5	5	5	**18**
10	5	5	5	4	4	**23**
11	2	1	3	3	2	**11**

12	5	5	5	5	5	**25**
13	1	1	4	4	2	**12**
14	5	5	5	5	5	**25**
15	2	3	4	4	1	**14**
16	5	5	5	5	5	**25**
17	5	4	2	1	5	**17**
18	5	4	5	3	3	**20**
19	5	4	2	2	2	**15**
20	5	4	5	5	5	**24**
21	5	1	5	5	5	**21**
22	5	2	4	4	3	**18**
23	5	3	5	5	5	**23**
24	3	3	2	2	1	**11**
25	5	5	5	5	5	**25**
26	4	4	2	1	1	**12**
27	5	5	5	5	5	**25**
28	2	1	5	5	5	**18**
29	5	5	5	4	4	**23**
30	2	1	3	3	2	**11**
31	5	5	5	5	5	**25**
32	1	1	4	4	2	**12**
33	5	5	5	5	5	**25**
34	2	3	4	4	1	**14**
35	5	5	5	5	5	**25**
36	5	4	2	1	5	**17**
37	5	4	5	3	3	**20**
38	3	3	2	2	1	**11**
39	5	5	5	5	5	**25**

40	4	4	2	1	1	**12**
41	5	5	5	5	5	**25**
42	4	4	1	2	3	**14**
43	5	4	4	4	4	**21**
44	5	5	5	5	5	**25**
45	3	4	4	4	4	**19**
46	4	4	2	1	1	**12**
47	5	5	5	5	5	**25**
48	5	5	5	5	5	**25**
49	4	4	1	2	3	**14**