DIGITAL FORENSICS FRAMEWORK FOR COMBATING CYBERCRIME

SUBMITTED BY:

WYCLIFFE MWATU

REG NO: 20/00977

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE REQUIREMENTS FOR THE AWARD OF A DEGREE IN MASTER OF SCIENCE IN DATA COMMUNICATION IN THE SCHOOL OF TECHNOLOGY AT KCA UNIVERSITY.

Declaration

I declare that this work has been completed according to the guidelines established by the faculty and has not been submitted for any other purpose.

Signature  13/10/2022.

Wycliffe Kelly Mwatu
Reg No:20/00977

This research has been submitted for examination with my approval as the University Supervisor

Signature  **Date 21st October 2022**

Supervisor Dennis M. Kaburu, PhD

ABSTRACT

Offenders use digital devices and networks to facilitate their crimes and hide their identities, Information technology systems are attacked creating new challenges for digital investigators. Malicious programs that exploit vulnerabilities also serve as threats to digital investigators. Since digital devices such as computers and networks are used by organizations and digital investigators, malicious programs and risky practices that may contaminate the integrity of digital evidence can lead to the loss of critical evidence. For some reason, digital investigators face a major challenge in preserving the integrity of digital evidence. Not only is there no definitive comprehensive digital forensics investigation framework for ensuring digital evidence reliability but there has to date been no intensive research into methods of doing so.

The aim of the study was to develop an efficient digital forensics framework for combating cybercrime. Additionally, the study aimed to assess existing frameworks used for combating cybercrime with a view to identifying existing gaps, develop an efficient framework for investigating digital crimes based on the universal standard for digital forensic investigation ISO/IEC 27043:2015 and finally validate the developed framework and evaluate its performance compared to other existing frameworks. The study utilized a quasi-experimental and descriptive research design and a target population of 105 participants which are officers drawn from the entire communication Authority digital forensics and investigation department.

The study concluded that digital forensic investigations require an efficient framework digital forensic examiners must adhere to a well-defined procedure that goes beyond technical requirements. As a result, we must examine previous efforts and forensic frameworks in depth. Therefore, a formal and methodical approach is required to provide a framework for analyzing and reasoning the requirements of digital investigations. In addition, anti-forensics situations and processes make the forensic investigation process challenging by contaminating any stage of the investigation process, its requirements, or by destroying the evidence.

ACKNOWLEDGMENT

This thesis would not have been possible without the guidance and help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

First and foremost, I would like to thank God the Almighty, for his showers of blessings throughout my research work. I have experienced your guidance day by day. You are the one who let me finish my degree. I will keep on trusting you for my future.

Secondly, am grateful to my supervisor, Dr. Denis Kaburu for his invaluable advice, continuous support, and patience during my study. His immense knowledge and plentiful experience have encouraged me all the time in my academic research and daily life. My gratitude extends to the KCA university school of technology for giving me the opportunity to do my research.

Finally, I am extremely grateful to my parents for their love, prayers, care, and sacrifices in educating and preparing me for the future. I am very much thankful to my wife and my daughters for their love, understanding, prayers, and continuing support to complete this research work over the past few years, it would be impossible for me to complete my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AI: Artificial Intelligence

CA: Communications Authority of Kenya

CIRT: Computer Incident Response Team

DBFIPM: Generic Database Forensic Investigation Process Model

DFMMIP: Digital Forensic Model based on Malaysian Investigation Process (DFMMIP)

GB: Gigabyte

GPS: Global Positioning System

IDFPM: Integrated Digital Forensics Process Model

NPKI: National Public Key Infrastructure

SDFIM: Systematic Digital Forensic Investigation Model

SMS: Short Message Service

SPSS: Statistical Package for Social Sciences

WCDFI: Wycliffe Comprehensive Digital Forensic Investigation Framework ()

LIST OF SYNONYMS

Model and Framework

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

The current technological revolution in communications and information exchange has created an entirely new form of computer crimes or cybercrime. Computer crime has forced the computer and law enforcement professional to develop new areas of expertise and avenues of collecting, analyzing and presenting evidence. This is what has evolved into the science of digital computer forensics. The process of acquiring, examining, and applying digital evidence is crucial to the success of prosecuting a cybercriminal. To effectively combat cybercrime, greater emphasis must be placed in the computer forensic (Gordon et al., n.d.; University of East London & Ay, 2020).

Most of the original needs assessments on the investigation of crimes involving digital evidence, only focus mainly general role of cybercrime investigations but the actual impact is less covered (Krishnan, 2019).As technology has improved, so has the way it is used in government, commerce, academia, and our personal lives. The potential value of high-tech devices has been recognized and their uses have been adopted by both criminals and investigators. There has been a constant requirement for updated tools, techniques, and methods that can be used for digital forensic investigations to address the increasing range of devices that contain either digital processors or digital storage media, as well as to address the complex environments in which they are found (*Role of Digital Forensics in Comberting Cybercrimes.*; Singh, 2014).

In the fight against crimes related to computers, digital forensics plays a crucial role. Digital forensics employs techniques for gathering probable evidence from digital devices, such as mobile phones, desktop computers, laptops, and server computers, in order to investigate alleged illegal or unauthorized activities (Crouch, 2012).Digital forensics have become more complicated as a result of technological advancements like the use of remote and distributed systems and artificial intelligence (AI), necessitating the development of a method that is both more dependable and applicable to all requirements now and in the future.(2019, Davies & Smith)

The number of suggested models and frameworks is rising, with each one focusing on filling in the gaps left by the previous ones. The majority of models agree that certain stages, such as preservation, collection, examination, and analysis, are important. Forensic researchers and practitioners adopt and use these stages to come up with new research perspectives to help fill in the gaps and address the ever-changing needs (Aziz et al.,2013).

Artificial intelligence is an important part of everyone's life in this digital age, where technology is constantly improving. The recovery, investigation, inspection, and analysis of data discovered in digital devices is the focus of the forensic science subfield known as digital forensics. It is frequently used to discuss mobile devices and computer crime. Private investigation and criminal law both frequently employ digital forensics (Marshall, 2021).

A rise in the number of people with internet access has resulted from the proliferation of personal computers and widespread internet use, which presents a number of challenges for digital forensics. Hacking tools are readily available. Because of the shortfall of unmistakable proof, the indictment is testing. A lot of capacity limit, estimated in Terabytes, confounds this request (Singh, 2014).Any technological advancement necessitates a solution upgrade or modification.

1.2 Statement of the problem

There has been tremendous change in Digital Forensic Investigation over the past twenty years. From the age of early computers to the current day mobile devices and storage devices, the crime rate has also followed this growth trend. The diverse nature of crimes, has seen the emergence of frameworks which get improved as time passes and therefore equip them with guidelines capable of handling crimes better.

Local research on digital forensics and investigations demonstrates that the field of forensic science faces numerous obstacles, including; has insufficient laws and policies to standardize forensic investigation due to skill gaps, inefficient frameworks, high costs, and inadequate infrastructure (Agarwal et al., 2011; Ieong, 2006; Kamble & Jain, 2015; Rahim et al.-a)

From a review of the existing frameworks, the researcher found out that a majority of the models lacked processes on that enforce a proper chain of custody when handling evidence and this is a fundamental aspect of cyber-crime investigation aspect. The researcher therefore seeks to

design a generic and efficient framework that improves the chain of custody during all stages of digital forensics. The framework will capture the vital information showing *what, who, when, where and how* evidence was handled thus proving the integrity of the evidence at all times. Further, the processes will be efficient in terms of cost and time taken when handling evidence will be easily applied in various branches of digital forensic investigations.

1.3 Main objective of the study

The purpose of this study is to develop an efficient digital forensics framework for combating cybercrime.

1.4 Specific objectives of the study

The specific objectives of this study are

i. To assess existing frameworks used for combating cybercrime with a view to identify existing gaps.
ii. To develop an efficient framework for investigating digital crimes based on the universal standard for digital forensic investigation.
iii. To design and evaluate its performance compared to other existing frameworks

1.5 Proposed solution

The researcher proposes to develop a generic framework that may be applied to most digital investigation procedures. Named as the Wycliffe Comprehensive Digital Forensic Investigation Framework (WCDFIF), its application will simplify the investigation process in a timely and accurate manner. The WCDFIF will enable practitioners produce more evidence when responding to an incidence response during the preliminary on-site classification of evidence as compared to other investigations process. Additionally, the framework will reduce the analysis time and while maintaining a proper and reliable chain of custody. The framework will provide a comprehensive number of processes that can be implemented in all jurisdictions, circumstances and devices. The WCDFIF integrates features of the Digital Forensic Model based on Malaysian Investigation Process (DFMMIP) (Sundresan Perumal, 2010) and the Systematic Digital Forensic Investigation Model (SDFIM) (Ankit Agarwal et al., 2011)

1.6 Research Questions

Specific questions of the study

i. Which existing frameworks used combating cybercrime and what are the prevailing gaps?
ii. Which is the best model for addressing cybercrime?
iii. To what extend the current address the performance compared to other existing frameworks

1.7 Significance of the study

The study is useful to the policy makers, academia and practitioners.

To the policy makers the study will be significant in identifying existing gaps and how to mitigate them. To the academia the study will contribute to existing knowledge in the area of computer forensics vis-à-vis cybercrime. To the practitioners the study will provide technological trends and status of digital forensics and appropriateness in addressing cybercrime.

1.8 Motivation

In recent years, there have been significant changes in the field of computer security. A number of new threats caused by technical, operational, and personnel-related challenges have seen digital forensics gain notable attention due to the increase in cybercrimes. Technical challenges include encryption, a huge volume of data, and incompatibility among diverse forensic tools. Operational challenges include incidence prevention, response, and detection. The most notable personnel-related challenge is the knowledge and skills in field of digital forensics for staff. Practice of use of digital technology in most organizations around the world has exposed them to cyber-attacks with ill-motivated actors devising malicious software and approaches together with online tools that can help them disrupt networks and systems and mine and steal as much information. Furthermore, cyber-crime has exposed security vulnerabilities and breaches that need the continued evolution of digital forensic frameworks and practices that can be used in legal proceedings. Therefore, the researcher seeks to find solutions that can help improve operations in the digital forensics field by analyzing existing frameworks and gaps in digital forensics.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

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

2.2 Digital Forensic

The dynamic world of technology has seen an exponential increase of digital devices that has led to the huge amount of data being inter-exchanged. Consequently, these digital devices are becoming more exposed and responsible for cybercrimes. Currently, more information is stored in its digital format than ever before. Important is the fact that digital investigators need clear, practical and workable processes that are in line with the laws and regulations of the country of operation and the evolving nature of digital investigations.

Digital crimes presented to court in face several admissibility challenges due to factors such as authenticity, poor documentation which lead to poor chain of custody, or reliability and in some instances, convincing the jury becomes an uphill task. Lack of standard principles and regulatory policies and with the ever changing technology make it difficult for practitioners to carry out their investigative duties. Very few colleges teach courses around the digital forensic field with a majority concentrating on theory rather that practical using real encounters.

Digital forensics plays a vital role in countering computer related crimes. Digital forensics uses investigation techniques that gathers probable evidence from digital gadgets including mobile phones, desktops, laptops and server computers for investigating suspected illegal or unauthorized activities (Crouch, 2012). The advancement of technology such as the use of remote and distributed systems and artificial intelligence (AI) has made digital forensic more complex leading to the need of a more reliable and universal method that will meet all current and future requirements. (Davies & Smith, 2019).

The number of recommended models and frameworks are on the increase with each building on managing the gaps presented by the existing ones. Most models agree on the importance of

some stages that include preservation, collection, examination, and analysis and forensic researchers and practitioners adopt and use these to come up with new research perspectives to help fill the gaps while addressing the in continually evolving needs (Aziz et al., 2013).

2.3 A Brief History of Digital Forensics Investigation

Since forensic science as a field was not widely discussed until recently, the history of the field needs to be investigated. One cannot help but increase one's admiration for this area of science when one becomes aware of the subtle significance of forensic science in the past. The Latin word "forensis," which refers to a forum, is where the term "forensic" comes from.Most of the time, forensic science is used in conjunction with any other field associated with the legal system. Simply put, forensic science is the application of scientific principles and methods to legal issues.

In ancient times, the location and method of the victim's discovery naturally assumed the manner of death.A man found in a body of water, for instance, would naturally have drowned, whereas a man found bleeding and broken on the side of the road would naturally have fallen and possibly been dragged by a horse.

When all else failed, torture was readily available to obtain a confession. Suspicion of motive and the word of others against a possible murderer took precedence over any other facts.

Midway through the 1980s, perhaps the most significant advancement in forensic science since the analog fingerprint was made: British geneticist, discovered in 1984 that evidence could identify family members with both similarities and differences, making it possibly the most accurate method ever discovered.

When local police were looking into the rape and murder of two women in 1986, they used Jeffreys' method for the first time in a criminal case: one that took place in 1983 and another that took place in 1986.Over 4,000 men in the area gave blood and saliva samples, but the method only found one match between the two crime scenes: Colin Pitchfork's .Pitchfork would not have been caught if . Importantly, however, it cleared Richard Buckland, who had previously been the prime suspect due to his false confession and who, according to authorities, would have served life in prison if it weren't for Jeffreys' contributions to the investigation.

Even though samples/artifacts alone is no longer sufficient to obtain a conviction, it continues to play an important role in forensic investigations. It has also been demonstrated to be as effective a method for determining innocence as it is for determining guilt, just like the initial case in 1986.samples/artifacts evidence helped clear Gary Dotson after he spent ten years in prison in 1989(Uon, n.d.).Since then, 375 samples/artifacts exonerations have been made. Thanks to Jeffreys' discovery, thousands of modern investigations have seen prime suspects identified and pursued, only to be found innocent prior to conviction.

2.4 Major Motivations of Cyber Criminals

a) *Financial Gain*

Gaining Money is a hacker's primary motivation. Threat actors target institutions with what they want, usually money, data they can sell for money, and data access vulnerabilities. According to (Broadhead, 2018), criminals are increasing the amount of reconnaissance they carry out each year in order to better target their victims in order to get the most out of their efforts and their chances of success. The financial sector will always be a prime target for cybercriminals due to its reliance on confidential customer data for business. Unfortunately, selling stolen personal information and credentials on the Dark Web does pay.

The business faces its own unique difficulties with mobile banking. Banks and other financial organizations must develop new technologies to meet the demand of customers who are increasingly relying on mobile applications to complete transactions. This raises their risk exposure and level.It is essential to note that the financial institution owns the risk, regardless of whether they use a proprietary or third-party mobile banking application. Mobile malware, third-party apps, unsecured wi-fi, and precarious customer behavior all pose a significant threat to mobile banking.

b) *Recognition & Achievement*

The satisfaction of successfully breaking into a significant system motivates some cyber criminals. Regardless of whether they work in teams or on their own, some people prefer to be acknowledged. This is also due to the fact that cyber criminals enjoy the challenge presented

by their actions and are naturally competitive. In point of fact, they frequently inspire one another to carry out hacks that are more difficult.

c) *Insider Threats*

It is simple for people who have access to important systems or information to choose to misuse that access in their organization's favor. These are thought to be some of the greatest threats to organizations' cyber security and can come from internal employees, vendors, a contractor, or a partner. Crowd Research Partners' Insider Threat Report, on the other hand, reveals that not all insider threats are premeditated. The majority are the result of carelessness, negligence, or compromised credentials; however, even in an unintentional situation, the potential impact remains.

Because the threat actor has legitimate access to the organization's systems and data, insider threats are difficult to identify. This is because an employee can't do their job well without access to resources like email, cloud apps, and network resources(Romagna, n.d.). Some employees will also require access to confidential information, such as financials, patents, and customer data, depending on the position.

Many security products would treat the behavior as normal and not issue any alerts because the threat actor has legitimate credentials and access to the organization's systems and data. As they become more complex, insider threats become harder to spot. A threat actor might, for instance, use lateral movement to cover their tracks and gain access to high-value targets. Or, as described below, an insider could take advantage of a system flaw to gain access(*Economic-Espionage-1.Pdf*, n.d.; *Irem_pdf_fbi_cyberthreats.Pdf*, n.d.; Romagna, n.d.).

An insider threat's ultimate objective is typically financial gain. Whether this is a malicious insider who has accepted cash in exchange for trade secrets, a negligent user who has received a spoofed email from an "executive" and sent a wire transfer to a fake bank account, or a compromised insider whose credentials have been stolen and used by attackers to infiltrate and sell patients' personally identifiable information (PII). However, there are numerous reasons why insider threats exist: sabotage, fraud, espionage, harm to a professional's reputation, or both(*CSS0080-Guide.Pdf*, n.d.).

d) *Political Motivation – "Hacktivism"*

Hacking skills are used by some cybercriminals to target large businesses. Most of the time, they are driven by a cause of some kind, like bringing attention to human rights or letting a large corporation know about system flaws. Alternately, they might encounter groups whose philosophies are at odds with their own. While these groups may steal information and claim to be exercising free speech, the majority of the time, they will use a DDoS (Distributed Denial of Service) attack to overcrowd a website and cause it to crash.

Hackers have presented a number of arguments claiming to justify non-malicious intrusions, which they believe are morally permissible. Some hackers, for instance, believe that these intrusions are justifiable from a consequential standpoint because they increase humanity's knowledge of relevant technologies and encourage the development of technologies that will ultimately contribute to making the Internet safer. Barriers that separate information on one person's computer from that on another computer are thought by some to be morally illegitimate and deserving of no respect (Samuel, n.d.).

Several issues , for instance ,political morality frequently prevents punishment for morally questionable actions.in this regard, mainstream political theorist believes that it would be morally permissible for the state to punish individuals for breaking unilateral promises (in contrast to an exchange of promises constituting a morally binding contract), despite the fact that it is presumably wrong to break any kind of promise. Moral standards in states and individuals frequently diverge; Thus, for example, court of law may legally sanction wrongdoing, but individuals may not. As a result, the fundamental characterization of the fundamental moral issues surrounding civil disobedience underpins the hacktivist argument(Romagna, n.d.).

on the other hand, and this is the most important point, it is immoral to inflict substantial harm based on a viewpoint that is fiercely contested in society, as is typically the case with digital civil disobedience. Keep in mind that, in comparison to digital civil disobedience, sit-ins and other forms of non-digital civil disobedience typically cause significantly less harm. A distributed denial of service (DDoS) attack against a large commercial website, for instance, could cost that site millions of dollars and possibly even the livelihoods of its users; Furthermore, it is difficult to see how the infliction of such harms on common people can be justified ethically as a form of free speech.

This is especially troubling because civil disobedience is typically motivated by a deeply contested moral viewpoint; in many instances, only a small number of people in the culture hold the viewpoint that inspires civil disobedience. There are moral restrictions on the kinds of harm or inconvenience that can be justifiably inflicted on people who are not morally responsible for the policy being protested because there is no reliable way to determine which side is correct. Hacking that can cause jobs to be lost is always a problem, but it's especially bad when it's based on ideas that haven't been properly defended, which is all too often the case(Romagna, n.d.; Rothke, 2001; Samuel, n.d.).

e) *State Actors*

A nation-state provides funding and assistance to actors sponsored by the state. They are specifically engaging in cybercrime to advance the interests of their nation. “Intellectual property, personally identifying information, and money to fund or further espionage and exploitation causes” are among the items that they typically steal. However, some actors with state sponsorship do carry out harmful cyber-attacks and assert that the cyber espionage they carry out is legitimate work for the state.

Before a cyber-attack, businesses need to act. An attack may leave some businesses financially crippled, resulting in the company's demise, which may prevent them from surviving(Rothke, 2001). Knowing which tools and strategies threat actors can use to target the company and then using this knowledge to their advantage is essential for cyber security. Organizations are less careful about who they allow into their systems than they are about what they let into the internet.Corporate spies have gained access to company computers by simply calling the systems administrator pretending to be an employee who has forgotten their username and password.

Cyber-attacks will continue to occur. Nation-state actors have the freedom to attack any nation with little investment thanks to high-speed networks and advancements in artificial intelligence. Understanding the fundamentals of cyber security tools will assist you in raising awareness of cyber security among all employees in departments other than IT(*Economic-Espionage-1.Pdf*, n.d.).

f) *Corporate Espionage*

A cyberattack of this kind is used to gain an advantage over a rival organization. Corporate espionage, which is carried out for financial or commercial reasons, entails for instance , theft of trade secrets, bribery, blackmail, or surveillance or acquiring property like processes or techniques, locations, customer data, pricing, sales, research, or strategies

The majority of businesses are somewhat cautious about what they let into the internet, but they are less careful about who they let into their systems. Simply calling the systems administrator claiming to be an employee who has forgotten their identify and password has allowed corporate spies into company computers. A corporate spy will enter a company and use an empty terminal if they know an employee is away, which is a little more complicated but still common. Memories from vacations, as well as bid prices, frequently end up in the trash(*Economic-Espionage-1.Pdf*, n.d.).

Infiltrators have as much access once inside as their computer skills permit. Because their profits depend on the exclusivity of their data, this kind of invasion could destroy research and development (R&D) businesses. Attention investors: Companies that cut back on research and development run the risk of saving money today but losing a lot of money later(Rothke, 2001).

Corporate spies are typically hired by businesses to spy on one another and can operate legitimate offices. A corporate spy might choose a company without being hired if business is slow, then gather information to sell to interested bidders. Although high-tech nabbing and stealing is done by hackers in some cases, most businesses have well-paid system administrators who are able to track digital spies (some of whom are former hackers).It is much simpler to track high-tech espionage than someone stealing garbage or calling the business with flattering questions .

The world of corporate according to (Rothke, 2001)espionage is very real and very unlike what one would think. Companies are concerned because it lacks gunfights and swift women and is far from glamorous. If a rival company doesn't get caught, knowing a competitor's next product line, bid price, or any other sensitive data can give them a competitive advantage. Corporate espionage will continue regardless of whether we learn about it because the temptation is strong(*Economic-Espionage-1.Pdf*, n.d.).

2.5 Success of Digital Forensic in Digital Crime Handling

Only when it achieves the desired outcomes can digital forensics be considered effective.The identification, collection, preservation, and analysis of information in a manner that preserves the integrity of the collected evidence for its effective use in a legal case is the primary objective of digital forensics. Each of the various capabilities of digital forensic tools has advantages and disadvantages.

In this digital age, technology is always getting better, and artificial intelligence is a big part of everyone's life. Digital forensics is a branch of forensic science that deals with the recovery, investigation, inspection, and analysis of data found in digital devices. It is often used to talk about computer crime and mobile devices. Digital forensics is frequently used in private investigation as well as criminal law (Marshall, 2021).

The proliferation of personal computers and widespread internet use have led to an increase in the number of people with internet access, which presents a number of challenges for digital forensics. Tools for hacking are readily available. Due to the absence of tangible evidence, the prosecution is challenging. A significant amount of storage capacity, measured in Terabytes, complicates this inquiry (Singh, 2014). Any advancement in technology requires a solution upgrade or modification.

From the perspective of mobile devices, the field of digital forensics has undergone significant transformation over the past ten years. Since the introduction of smartphones (the first iPhone was released in 2007), phones have undergone significant transformations (*IPhone History - Complete History of IPhone - IPhone Alley.Htm*, n.d.). At the start of this era, phones were typically designed to store only a small amount of contact information (primarily a short name and a number), make and receive calls, and send and receive SMS messages, all with a small amount of storage space. From contacts, calls, and messages (which include standard SMS, application messages, multimedia messages, and emails) to media files like music, images, and documents, today's smartphones can store a lot of data (*A Brief History of Forensic Science - MozartCultures -Now.Htm*, n.d.; *IPhone History - Complete History of IPhone - IPhone Alley.Htm*, n.d.; *IPhone History - Complete History of IPhone - IPhone Alley.Htm*, n.d.). With smartphones that can store data in 512GB and memory cards that can store an additional 1024GB, there could be 1.5TB of storage. Users can now communicate outside of standard networks, send encrypted data, and automatically destroy messages and images with a wide

range of free and paid applications. To provide organizers, navigation tools, file sharing tools, IoT (Internet of Things) controllers, document processing, health application data, etc., apps also interact with on-device cameras/video recorders and GPS locators.

Digital forensics can be a costly endeavor that requires licenses, expensive equipment, and significant personnel costs. In order to gain the support of the command staff, it is essential to demonstrate a reasonable return on investment.

There are a lot of digital evidence backlogs, a lack of equipment, and the possibility of examiner turnover in departments. The lack of personnel trained in digital evidence extraction adds to the backlog. Because classes would take examiners away from the workplace, a growing backlog prevents training opportunities. Additionally, a backlog can undermine requests to replace licenses and technology that is inadequate, out-of-date, or underfunded due to budget constraints of units that are perceived to be performing slowly(Broadhead, 2018).

As earlier indicated, Digital forensics and investigations can be a costly endeavor that necessitates expensive several licenses to enable them to run, complex equipment, and substantial staffing costs. It is essential to demonstrate a reasonable return on investment in order to gain the support of the command staff.

2.3.1 Digital Crime Handling

Digitally stored data is very sensitive and can easily get lost. It is important to use best practices to properly seize devices and computers. Firstly, the scene need to be secured and permission granted by legal authority to seize the evidence confirmed. This can be through a court order to search and collect evidence from the identified crime scene.

Businesses and other private individuals have become targets for cybercriminals as the economy has shifted from traditional processes to the internet in Kenya and around the world. The CA's cyber report shows that attempted cyberattacks decreased from 143,040,599 between July and September 2021 to 79,175,429 between January and March 2022.Kenyan law enforcement partners with the CA to respond to and respond to cybercrime in the fight against it.By establishing a national Computer Incident Response Team (CIRT), CA was required to develop a national framework for cyber security management in accordance with the Kenya Information and Communication Act of 1998.Despite the enormous opportunities presented by

digitization, it is essential to be aware of emerging risks due to the severity of the threat. The Central Bank of Kenya recently advised Kenyan businesses to be extra vigilant against the growing threat posed by cybercrime, noting that such attacks are likely to become more frequent. Cybersecurity continues to expand rapidly as more citizens enter the digital realm. Personal data continues to accumulate as the pandemic accelerates global economic digitization. Therefore, in order to safeguard our citizens, we must ensure adequate safeguards exponentially.

The response team's responsibilities include the development and implementation of a National Public Key Infrastructure (NPKI), the timely mobilization of various actors locally and internationally to respond to cyber incidents, the implementation of national cybersecurity policies, laws, and regulations, cybersecurity awareness and capacity building for the general public and forensic practitioners, and research and development in cybersecurity (Communications Authority of Kenya, n.d.).

Criminal investigations, prosecutions, and judicial representation all rely heavily on the handling and interpretation of digital evidence. Professionals who rely on digital evidence must keep up with developments in technology. Digital forensics experts in the United States have developed new digital forensic investigative techniques as a result of the rapid growth of digital technology and the evolution of privacy and search and seizure laws. I need to develop a tool (Agarwal et al.,2011).According to Kamble & Jain (2015), the group looked for digital forensics best practices that could be used right away in their investigations. They also found gaps and requirements on which to base their training materials.

2.3.2 Effectiveness of Digital Forensic in Kenya

Earlier passed laws on computer and digital forensics often become outdated making it difficult to effectively assess the procedures used in this field of study. This poses a challenge to the extent of usage of computer forensics evidence in the court. There has been slow progression of digital forensics in Kenya due to lack of adequate regulatory policies, ethics, actions and technologies. Need to say there is an urgent continuous need for the law to keep pace with the advancement of the technology. Another challenge prohibiting the effectiveness of digital

forensics in the country is the lack of adequate training. With the changing technology investigators need realize that the role technology plays in almost every crime and therefore all actors especially the police departments need to adapt to the changing times and prepare for cybercrime by understanding how cybercrimes are committed and how to tackle the crimes (Odoyo et al., 2020). Additionally, the lack of adequate training can lead to tampering of evidence leading to court dismissals.

When getting better and reading information from the victim's virtual tool(s), investigators have to adhere to suitable methods so as for virtual proof to be admissible in the courtroom docket.

In a few instances, the usage of computer forensic proof in courtroom dockets is restrained because of the regulation's incapacity to hold up with technological advancements. Computer forensics professionals aren't constantly consulted earlier than writing a number of those legal guidelines, and they may be often now no longer reviewed; now no longer dependable sufficient to assess the strategies of a virtual system/tool search.

The "Cyber-crime and Computer-Related Crimes Bill" from Kenya turned into the concern of a completely thrilling prison evaluation with the aid of using Article 19.It is apparent from their very last document and guidelines that those payments and legal guidelines concerning the usage of virtual proof in courtroom dockets have to be reviewed. Legislators, regulation enforcement organizations, and privacy advocates want to bring collectively to expand powerful Standard Operating Procedures (SOPs) for forensics examiners and legal guidelines that could aid honest and independent trials.

Before creating a decision, our prosecutors and attorneys have to realize those forensics strategies for obtaining virtual proof and be capable of asking important questions. On the opposite hand, our regulation faculties want to deal with a number of those troubles with the aid of using going over their path paintings and giving the scholars an advent to virtual forensics.

Our legislators and judges should obtain schooling as a way to help regulation enforcement organizations in preventing associated crimes. When our judges have enough facts concerning a case and the proof presented, we will best attain an honest verdict. Our regulation enforcement organizations want the right to get the right of entry to the maximum current forensic

equipment, hardware, and devices as a way to enhance their investigative talents and grow to be a dependable supply of virtual proof. There is a lot to research given the brand new smartphones, tablets, and different gadgets being launched to the general public with the aid of using competing hardware production companies, in order that they must obtain new schooling a minimum of two times a year(Uon, n.d.).

Concerns approximately privacy are any other trouble while managing forensics. There is a first-rate line between what forensics must contain and what a suspect's human rights are. For instance, if a suspect's smartphone is seized, a brand new SMS is sent. Should or should not the brand new message be appeared? There are privacy advocates who will argue that that is a contravention of human rights. Additionally, generation may also be used to help criminals in hiding their movements because the availability of loose encryption and anonymity equipment and talents grows.

Legislators and regulation enforcement organizations must expand guidelines, protocols, and methods to deal with those troubles. They should make clear conflicting legal guidelines that would save you the usage of virtual proof in courtroom docket and set up popular strategies for obtaining proof. These methods and guidelines should be independent(Kilungu, n.d.).

2.4 Gaps in the Literature

From the literature, it is clear that there are several factors that affect digital evidence acquisition, handling and presentation as a result jeopardizing the efficiency and effectiveness of cyber forensics investigations. Firstly, proper acquisition and handling of evidence plays a vital role in determining the outcome of the analysis. Lack of proper guidelines for the acquisition and presentation of electronic evidence may ruin or alter the evidence nature.

Secondly, the lack of enough digital evidence expert in various agencies the officer also poses a threat to the success of digital forensics. The presence of limited and outdated formal training centers and standardization makes a number of the practitioners learn on the job, with the wide array of the digital forensic sectors posing a limitation. For example, techniques used in handling electronic evidences from bank frauds differs from those used to handle evidence from social media or mobile phones. Thirdly, most practitioners are presented with low budgets and limited resources. Technological choices impact the cost incurred while handling digital

forensics. Some frameworks employ expensive tools and software's limiting some agencies into using those that are free to download.

The volume to which regulation enforcement employs digital forensics technique and equipment, their implementation of digital forensics recommendations and standards, and the acquisition, exam, and evaluation of virtual facts asses are the challenge of inadequate research. It is unknown how investigative reviews preserve stages of the chain of custody with a view to having a look at the digital forensic exam that changed achieved in every case.

As the era of digital forensics advances, so do criminals and their methods. In virtual forensics, this system is known as the Anti-forensics technique, and it's far appeared as a chief assignment within side the digital forensics world. While criminals use such equipment to hide, alter, or dispose of the lines in their crime, digital forensic specialists use forensic equipment to gather shreds of proof in opposition to criminals.

Because virtual proof is greater touchy than bodily proof and might effortlessly vanish, it's far greater tough for a virtual forensic professional to investigate such huge quantities of facts as crime quotes rise. Digital Forensic specialists use a number of equipment to confirm the authenticity of the facts with a view to expedite and advantage the investigation. However, the use of those pieces of equipment is an assignment in and of itself.

2.5 The Future of Cybercrime

Cybercrime Forensic investigation is a complicated field with its own past, repercussions, and prospects. It is not sufficient to simply classify it as a subfield of criminology, the study of cybercrime, or research into the connection between tech-related crime and social policies. The crimes and knowledge of cybercriminals are intertwined. The potential suspects possess a wealth of technical and knowledge expertise(Raghavan, 2013). They know how to use technology in opposition to technology and have mastered it better than its creators. To fully predict the future of cybercrime forensics, a multidisciplinary approach is required. It requires a team of experts from the IT industry, as well as related industrial and social sectors like telecom and law(Ieong, 2006).

As a result of the, evidence collected is now dispersed across a variety of physical and virtual locations, such as online social networks, cloud resources, and personal network-attached

storage units. explosion of complexity(*A Brief History of Forensic Science - MozartCultures - Now.Htm*, n.d.; Kilungu, n.d.; Rogers & Seigfried, 2004; Uon, n.d.). As a result, more knowledge, resources, and time are required to accurately and completely reconstruct evidence. The digital investigation community has voiced their strong disapproval of partially automating certain tasks because doing so could quickly lower the quality of the investigation (Aziz et al., 2013; Ieong, 2006; Marshall, 2021; Uon, n.d.).

Standards development they add that cutting-edge cybercrime investigations may necessitate outsourced storage and computation or collaborative processing of information. As a result, the creation of appropriate standard formats and abstractions will be an essential step for the digital forensics community.

Privacy-preserving investigations in today's world, people share many aspects of their lives online, primarily through social media sites or online social networks. Unfortunately, when cloud computing is involved, gathering information to reconstruct and locate an attack can severely violate users' privacy.Legitimacy technological Infrastructures of the present day are becoming increasingly complex and virtualized, frequently shifting their complexity at the border of fog computing or delegating particular tasks to third parties that is platform-as-a-service frameworks (Almarzooqi & Jones, 2016; *Role of Digital Forensics in Comberting Cybercrimes.Pdf*, n.d.; Singh, 2014)**.**

Evolution of the development of anti-forensics methods Encryption, obfuscation, and cloaking methods, which include hiding information, are examples of defensive measures. Despite international jurisdictional cooperation, it is essential for law enforcement to investigate cybercrime and gather evidence in order to build solid cases. Security professionals need the best investigation equipment for this(Raghavan, 2013).

"Digital forensics is essential to investigations that are carried out in a setting that is frequently closely linked to its cyber extension. Cybercrime and fraud in today's digital societies can result in financial losses or dangers for individuals. As a result, the upcoming generation of forensics tools ought to be designed to support diverse investigations, safeguard privacy, and provide scalability(Rogers & Seigfried, 2004).

Using a combination of intelligent tools and digital forensics procedures, the investigation of cyber-attacks has evolved more than ever before. Because they are not attack-agnostic, intelligent tools like FTK rules and Indicators of Compromise are only effective when there is prior knowledge about the software and mechanisms used in the cyber-attack(University Of East London & Ay, 2020). As a result, the number of novel software and mechanisms utilized is inversely proportional to the effectiveness of these intelligent tools. Even though digital forensic procedures do not have this problem, they are unable to provide comprehensive support for an investigation into a cyber-attack. The reason for this is that the examination and analysis phases of the processes where the actual investigation takes place lack sufficient details(Gordon et al., n.d.).

2.6 Digital Footprints and Forensic Investigations

For fraud investigators, the increasing reliance on technology in all its forms is both beneficial and detrimental. An ocean of data that can serve as crucial evidence in an investigation is presented by the exponential growth of a person's digital footprint as they move through life. However, acquiring, processing, and analyzing that data can be intimidating(University Of East London & Ay, 2020).

Every action leaves a digital footprint, regardless of how technologically advanced, inventive, or devious a fraudster is. Nearly every waking moment and frequently even while asleep, humans contribute to their digital footprint. Nearly everything we do contributes to our digital footprint, from traditional sources of information like text messages, emails, and online search history to information shared with apps on our mobile devices and smartwatches like sleep patterns, geolocations, and activities(Almarzooqi & Jones, 2016). This digital footprint is extremely valuable to investigators, con artists, and marketers alike. It is especially useful for making fraud investigations easier to conduct and more accurate, as well as for increasing confidence in the conviction of criminals. When conducting an investigation into fraud, acquiring, analyzing, and interpreting electronic evidence is no longer a luxury but rather a necessity. There are very few cases in which electronic evidence, whether structured or unstructured, must be collected and analyzed.

Investigators are now able to connect the dots thanks to the digital trail left behind by individuals who post on or even view various social media platforms—something that was

previously impossible. On social media platforms, people typically share too much information or media that contains data points that are not immediately apparent to the user(Singh, 2014).

2.7 A Digital Forensic Investigation Forensic Traceability Index

With the advancements in modern computers, networks, and the availability of a variety of digital devices, digital crime has become so sophisticated that it is difficult to trace its sources or origins. Digital crime causes enormous harm to users and systems. Using scientific methods, techniques, and investigation frameworks, forensics plays a crucial role in facilitating investigations of illegal activities and inappropriate behaviors. Digital forensics was developed for the purpose of examining any digital devices used in the prevention of crime.

2.8 Ecosystem spaces for cybercriminals

To comprehend how the criminal underworld's phenomena have developed over time, black market analysis is essential. When dealing with the criminal underground, the first thing to take into consideration is its fragmentation. Criminal organizations tailor their offerings to the market they target; security experts have even observed significant differences between groups operating in different nations(*ITU Seminar 15.05.18 - Oleksandr Potii.Pdf*, n.d.).

For communities of cyber criminals, black markets are the most significant points of aggregation on the deep web; they are an exclusive location where the criminal offer meets an even more specialized demand.

The anonymity afforded by the Internet, particularly the Deep Web, is used by cybercriminals from all over the world to hide from law enforcement. The level of penetration of each underground market into the Deep Web is influenced by differences in infrastructure and skill(Broadhead, 2018; “[No Title Found],” n.d.; “[No Title Found],” n.d.; Samuel, n.d.).

Cybercrime has become more organized; since there are complete criminal supply chains, hacking has become significantly more sophisticated and risky. For instance, cybercrime organizations manage more than half of all attacks and are better organized than most businesses. They have chief executives, account managers, and dedicated call centers that assist ransom-paying victims. Theft of data and extortion are their main sources of income. One of the main reasons the cybercrime industry continues to expand rapidly and earns more than one

trillion dollars annually is because of their Cybercrime-as-a-Service ecosystem. One illustration of this kind of increasingly well-organized cybercriminal operation is Dark Side(Rothke, 2001).

2.4.1 Computer Forensic Process

The Computer Forensic Process (Feng, Dawam & Amin, 2017) is one of the most recent frameworks that was designed and used a non-invasive mechanism to collect and store sensor data whenever accidents involve autonomous vehicles in smart cities. Despite the fact that the framework is efficient, secure, and preserves the integrity and privacy of data generated by the vehicles in question, the framework's application is costly in terms of use of advanced Communication technology and software used. It is also limited to use in smart cities thus diminishing the geographical area of operation. Secondly, it is can only be used in computer based forensics.

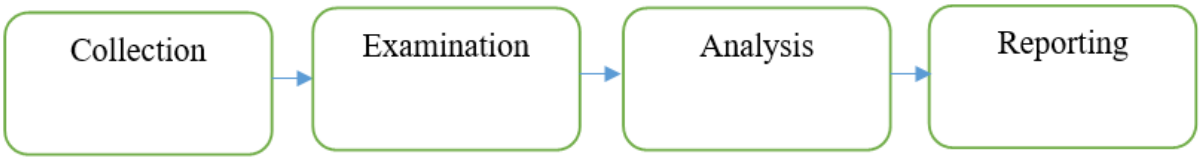


Figure 0:1 Computer Forensic Process

Source: Researcher

2.4.2 Generic Database Forensic Investigation Process

The Generic Investigation Process proposed by (Al-Dhaqm et al., 2016) tried to address gaps found in forensic investigations involving database systems. The proposed framework Generic Database Forensic Investigation Process Model (DBFIPM) proposed five stages namely the identification, collection, preservation, analysis and presentation process. The DBFIPM aimed reconciling concepts and terminologies commonly used in databases forensic investigation processes. This model expected to help investigators examine crime cases related to database contents, data files, metadata, memory data and log files in order to create a sequence of events, relationship or recover relevant data to be used as evidence. Just like the name suggests, a generic framework is ambiguous as steps are not well defined thus time consuming. Additionally, it is only suitable to cases that involve databases leaving out other forensic fields.

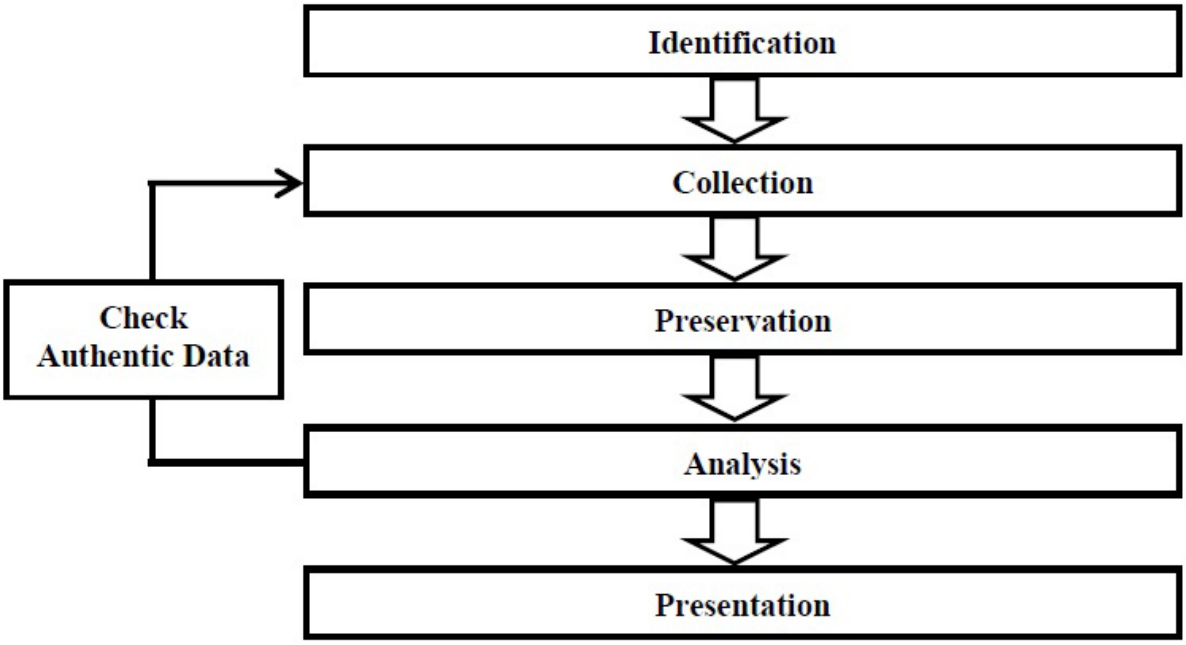


Figure 2:2 Generic Database Forensic Investigation Process

Source: (Al-Dhaqm et al., 2016)

2.4.3 Integrated Digital Forensics Process Model

(Kohn et al., 2013) developed an Integrated Digital Forensics Process Model (IDFPM) that proposed the use of a standardized framework to help investigators follow a uniform approach in digital forensic investigations. This framework tried to put together processes and sub-processes previously suggested. The framework has 4 main stages with each having a number of sub-stages. The six stages include Preparation, Incident, Incident Response, Physical Investigation, Digital Forensics Investigation and Presentation.

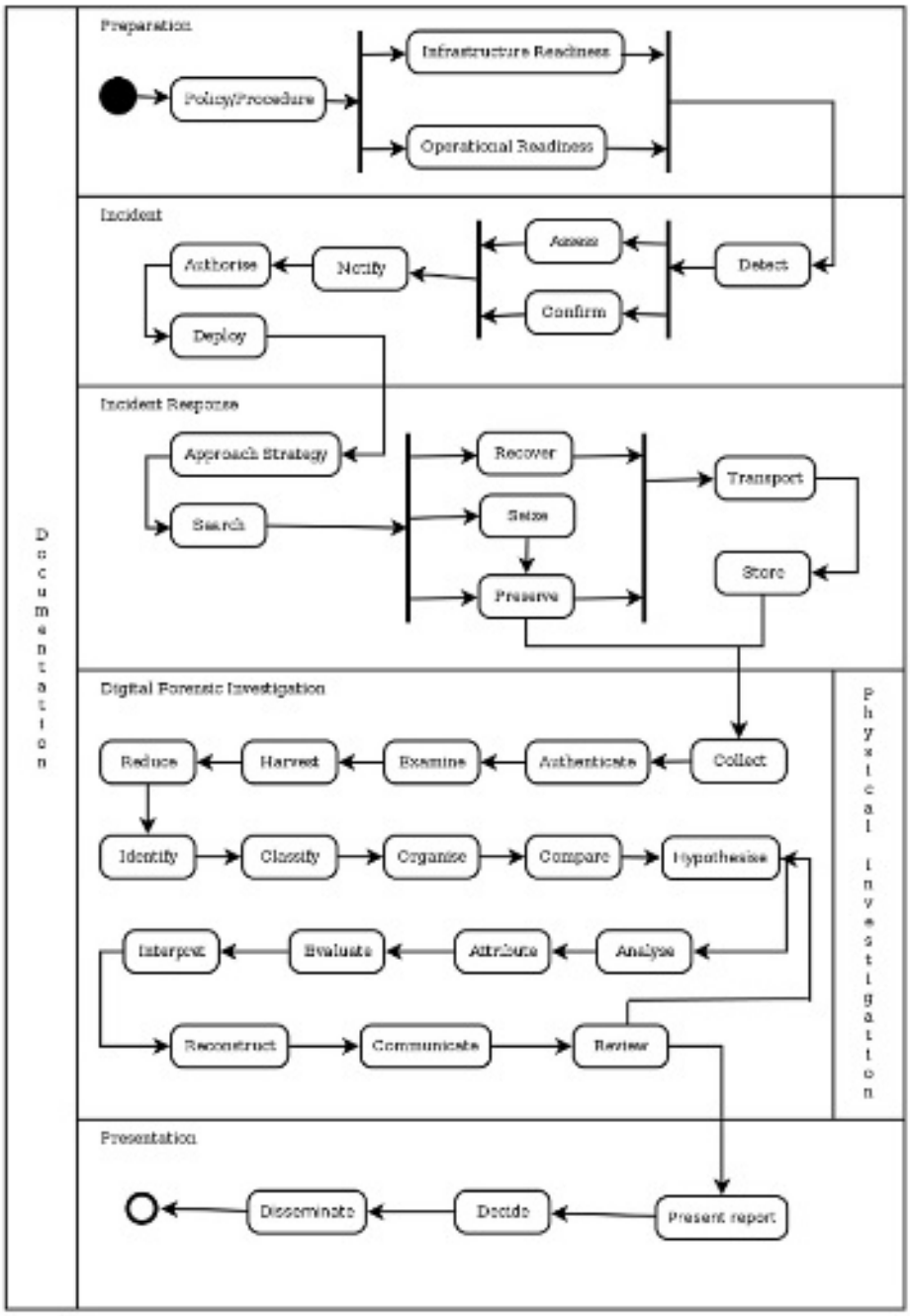


Figure 2:3 Integrated Digital Forensics Process Model

Source: (Kohn et al., 2013)

2.4.4 Systematic Digital Forensic Investigation Model

(Ankit Agarwal et al., 2011) developed a standard framework that was systematic and incorporated a mechanism that could incorporate a country's digital forensic processes and methodologies used by the jury while analyzing cybercrimes. The SDFIM was inspired by the inspired from the DRFWS Digital Investigation Model, and had 11 stages namely; Preparation, Securing Scene, Survey & Recognition, Documentation of Scene, Communication Shielding, Evidence Collection, Preservation, Examination, Analysis, Presentation Then Result & Review. The limitation with this is that the framework can be complex and time consuming to a team with little or no expertise or when applied in a country that lacks standard digital forensic investigation policies.

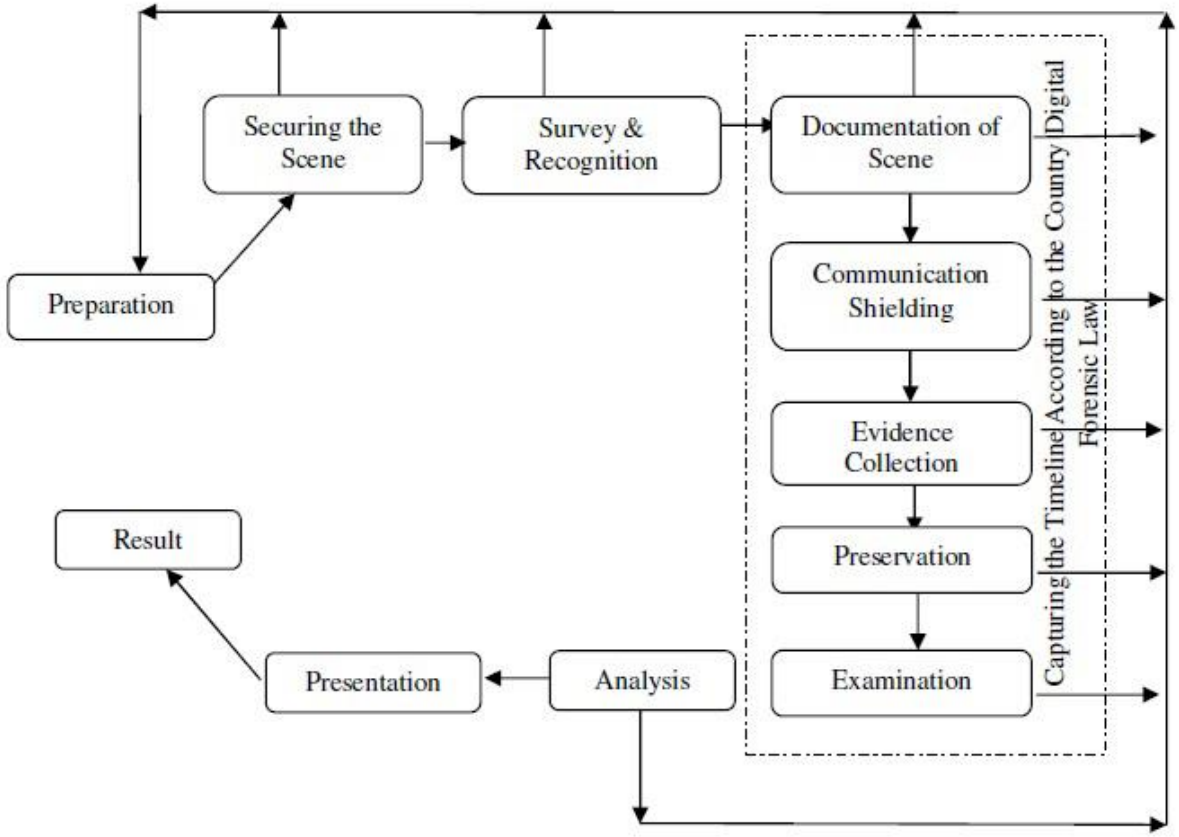


Figure 2:4 Figure 2.4.4: Systematic Digital Forensic Investigation Model

Source: (Ankit Agarwal et al., 2011)

2.4.5 Digital Forensic Model Based On Malaysian Investigation Process

Digital Forensic Model Based on Malaysian Investigation Process developed by (Sundresan Perumal, 2010) was a law specific framework based on the Malaysian Cyber laws. Malaysia saw an increase in computer crime and the criminal justice lacked standard procedures in the collection of electronic evidence. They also lacked proper guidance on the procedures for forensic investigator necessary to ensure the efficiency, accuracy and how to preserve the fragile evidence. This model has seven stages namely; Planning, Identification, Reconnaissance, Transport and Storage, Analysis, Proof and Defense, and Archive Storage. This framework is mostly useful to the Malaysian court proceeding and applying it to different jurisdictions might be time consuming especially when there is a need to align it to the practices of the said county.

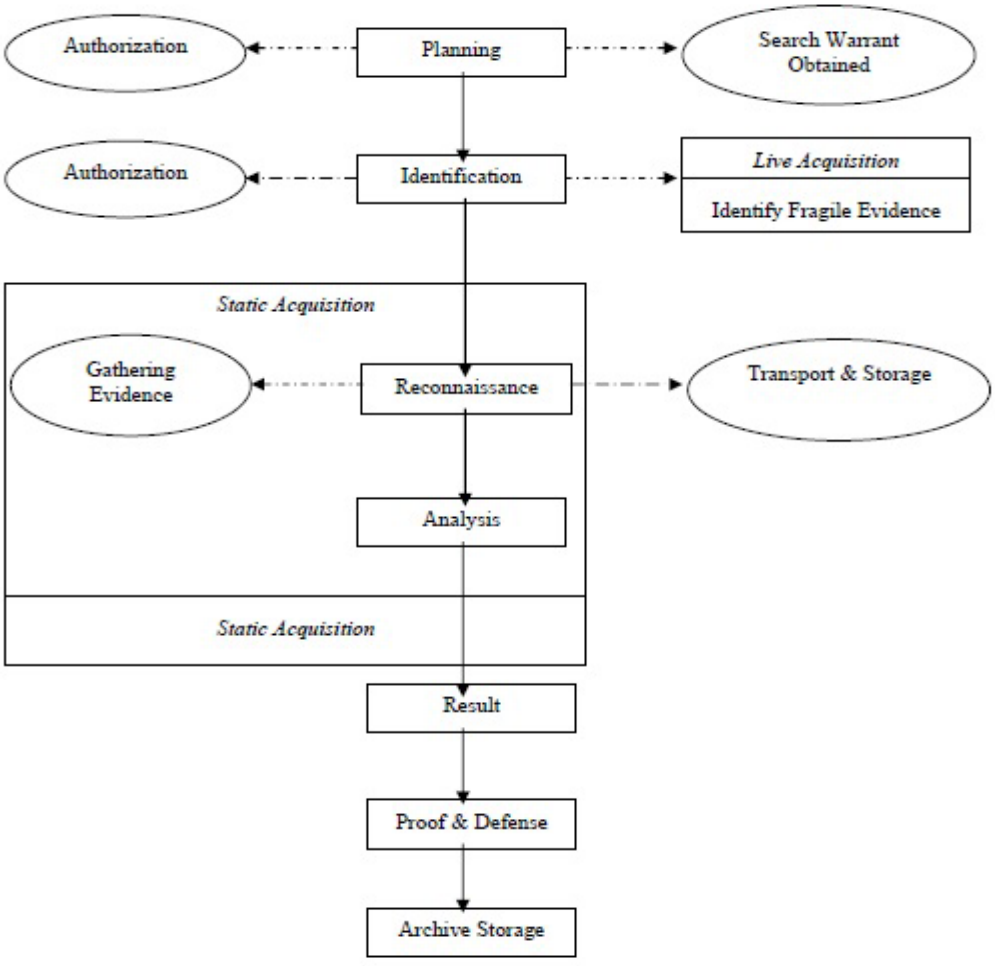


Figure 2:5 Digital Forensic Model Based On Malaysian Investigation Process

Source: (Sundresan Perumal, 2010)

So much research that has been done concerning suitable digital forensics investigation frameworks. However, minimal focus has been put towards the use of digital forensic to conduct a comprehensive investigation especially when it comes to advanced system and systems that have fully migrated to the use of latest technology such as cloud computing and Internet of Things. An analysis on a few of the earlier developed frameworks shows the lack of standardization of processes leading to gaps that interfere with the outcome of digital crime cases. There is a need to have standard processes and methods that can be adopted to similar cases internationally. ("ISO/IEC 27037:2012 Information Technology Security Techniques Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," n.d.).

Therefore, there is a need for practitioners to adapt to reliable frameworks while conducting digital forensics investigations. Such a framework should address the tools and methods needed while taking into consideration of parameters around time, cost and resources that often pose as critical constraints in an investigation. This research addressed the aforementioned gaps by proposing a systematic framework that standardizes the technical and legal requirements to improve and ensure the admissibility of digitals evidence during legal proceedings.

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
Computer forensic process-framework	Feng, Xiaohua Dawam, Edward Swarlat and Amin, Saad	2019	4	Collection, Examination, Analysis and Reporting	Costly due to smart technology used and is limited to smart cities
Generic investigation process - framework	Arafat Al-Dhaqm, Shukor Abd Razak, Siti Hajar Othman	2016	5	Identification , Collection, Preservation, Collection, Analysis and Presentation	The model is not exhaustive with respect to other forms of

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
	and Asri Nagdi				digital technologies. Eg: Cyber computing, Internet of Things (IoTs), etc. Time consuming and not effective
Intergrated Digital Forensics	Kohn, Ellop, M.M, J.H.	2013	6	Preparation, Incident, Incident Response, Physical Investigation, Digital Forensics Investigation and Presentation	Poor database /g of

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
Process Model					processed data
The Systematic Digital Forensic Investigation framework	Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta	2011	11	Preparation, Securing Scene, Survey & Recognination, Documentation of Scene, Communication Shielding, Evidence Collection, Preservation, Examination, Analysis, Presentation Then Result & Review	Complex, not effective and time consuming
Digital Forensic Model Based on Malaysian Investigation Process	Perumal	2009	7	Planning, Identification, Reconnaissance, Transport and Storage, Analysis, Proof and Defense, and Archive Storage	Country Specific based on Malaysian laws

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
Investigation process framework	Felix C. Freiling , Bastian Schwittay	2007	3	Acquiring Evidence Examination Analyzing Evidence	The framework is silence on the presentation and admissibility of the evidence in the court of law
Investigation framework	Michael Köhn, M. Olivier, J. Eloff	2006	3	Acquiring Evidence Authenticating Evidence Analyzing Evidence	

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
Computer forensic field triage process framework	Marcus Rogers, James Goldman and Rick Mislan	2006	4	Identifying, Preserving, Analyzing and Documenting	
Forensic process	Karen Kent, Suzanne Chevalier, Timothy Grance, and Hung Dang	2006	4		
Enhance integrated digital	Baryamureeba & Tushabe	2004	21		

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
investigation process - framework					
Extended model of cybercrime investigation process - framework	Séamus Ó Ciardhuáin	2004	13		
Hierarchical, objective based framework	Nicole Beebe and Jan Guynes Clark	2004	6	Preparation, Incident Report, Data Collection, Data Analysis, Findings presentation, Incident closure	
Event Based Digital Forensic	Brian Carrier and Eugene	2004	16		

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
Investigation Framework	H. Spafford				
An integrated digital investigation process - framework	Brian Carrier and Eugene H. Spafford	2003	17		
End to End digital investigation	Peter Stephenson	2003	9	Collecting Evidence, Analysis of individual events, Preliminary Correlation, Event normalization, Event confliction, Second level correlation, Timeline Analysis, Chain of evidence construction, Corroboration	
Abstract model of the digital	Mark Reith, Clint	2002	9	Identification, Preparation, Approach Strategy, Preservation,	

Framework	Inventor	Year of Invention	Number of stages	Key features	Gaps
forensic procedures	Carr, G. Gunsch			Collection, Examination, Analysis, Presentation, Returning Evidence	

Table 2:1Comparison of different frameworks

Source: Researcher

.

2.7 **Conceptual Other gaps above mentioned frameworks**

Several aspects of technology have been software and hardware. For instance, significant advancements in mobile device hardware have made it possible for these devices to efficiently carry out intricate operations. In parallel, the software that runs on mobile devices has also undergone significant development to meet consumer demand. However, digital forensic methods, particularly those that were developed around a particular set of technologies, have been impacted by these enormous technological shifts.p.Selamat and co. According to (2008a), numerous digital forensic techniques have been developed to target specific devices or types of technology. The underlying technology's rapid evolution renders these methods obsolete, which is the primary issue with them.

In view of the above, Different legal systems have different views of digital forensics, which has an impact on the methods used by forensic practitioners in those countries. According to Perumal (2009), "There is a little consistency and standardization in the court and industry sector as computer forensic is a new regulation in Malaysia."Therefore, it is not yet recognized in Malaysia as a formal "Scientific" discipline" (p. 40).As a result, jurisdictions that lack a comprehensive understanding of computer forensics and the procedures used to preserve and analyze electronic evidence will be most affected. Additionally, the legal system's lack of comprehension would lessen its influence on the development of methodologies and their acceptance by legal standards.

The researchers who create these frameworks have also contributed to one of the additional difficulties associated with digital forensic methodologies. Non-digital forensics-related titles and terms have been used by some researchers to describe their frameworks. Baryamureeba and Tushabe (2004), for instance, referred to the fourth stage of the EIDIP Model as the Dynamite Phase, which includes the sub phases of communication and reconstruction. Any effort to assist groups outside of the digital forensic field in better comprehending the digital forensic field's procedures would be hindered by this ambiguity in terminology. Digital forensics and the evidence gathered from an investigation using digital forensics are still poorly understood in some jurisdictions around the world, as previously stated. As a result, researchers would benefit from speaking in terms that are less technical and more common when discussing digital

forensic techniques. The legal system would gain a better understanding of digital forensic procedures with this simplified terminology.

2.8 **Conceptual framework**

A conceptual framework defines relevant variables of the study and shows how they are linked to and support one another for a comprehensive understanding of the phenomena in question. Dependent variables are 52variables whose variations depend exclusively on the independent variables. Dependent variables check the effects of the independent variable on the target sample. Independent variables are those whose disparities do not depend on other variables.

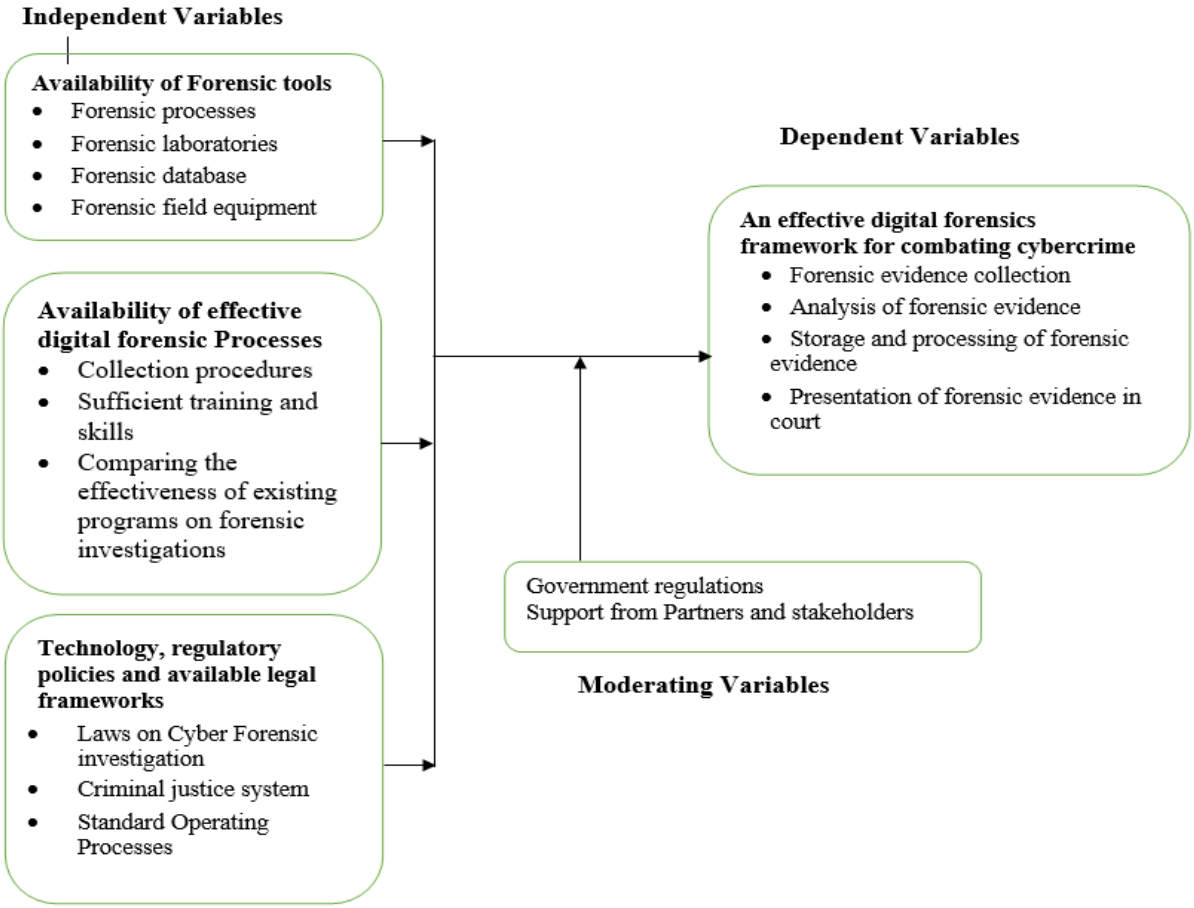


Figure 0:2Conceptual Framework

Source: Researcher

2.8 Proposed Framework

The proposed WCDFIF considered the Malaysian investigation process because it permits on-site analysis of digital device. Secondly, the model is time conscious since less time is required to handle the device under examination with less interruption to organization's operations. And thirdly there is no need to interfere with the device's location by transporting it to the lab since evidence collection and analysis is done on-site. The Systematic Digital Forensic Investigation model was considered because firstly, it addresses the issue of information flow and therefore looking into evidence dynamics and reconstruction of events thus upholding the crucial properties of Confidentiality, Integrity and Accountability necessary while analyzing computer frauds and cybercrimes. Secondly, the processes present offer generalized solutions that can be easily applied in the rapidly changing and highly unpredictable digital technological scenario. Lastly, it allows a proper chain of custody when handling evidence thus ensuring the integrity and admissibility of digital evidence in court processes.

The WCDFIF framework processes has 6 major phases with each having progressive sub-stages. The stages are named as Planning, Identification, Collection, Examination, Reconstruction, and Presentation. Planning has two sub-stages named that entails understanding and documentation of reason for investigation and obtaining a search warrant from the relevant authorities. Identification involves the identification of the type of evidence, pinpointing the location of the evidence and knowing where it is stored and also identifying the storage format. Collection necessitates the securing and preservation of the evidence, the actual collection of the evidence if need be, the appropriate storage and transportation of evidence to a secure and accessible location by authorized personnel. Examination involve the creation of an image of the evidence, analysis of the evidence to validate the reasons of investigation and the creation of hash values. Reconstruction enables the recreation of evidence with the aim of identifying connections between evidence, sequence of events, unearthing the identity of those involved as well as looking for missing or additional pieces of the evidence. Finally, Presentation involves the documentation of findings and reporting in a format that is easily understandable by both experts and lay persons.

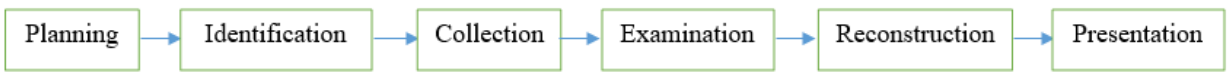


Figure 0:3Wycliffe Comprehensive Digital Forensic Investigation Framework (WCDFIF)

<table>
<tr><th colspan="2">Systematic Digital Forensic Investigation Model (SDFIM)</th><th colspan="2">Digital Forensic Model based on Malaysian Investigation Process (DFMMI)</th><th colspan="2">Wycliffe Comprehensive Digital Forensic Investigation Framework (WCDFIF)</th></tr>
<tr><th>Stage</th><th>Sub-Stage</th><th>Stage</th><th>Sub-Stage</th><th>Stage</th><th>Sub-Stage</th></tr>
<tr><td rowspan="2">1. Preparation</td><td>Authorization and search warrant</td><td rowspan="2">1. Planning</td><td>Authorization</td><td rowspan="2">1. Planning</td><td>Understand and document reason for investigation</td></tr>
<tr><td>Preparation of investigation strategy</td><td>Obtaining search warrant</td><td>Obtain search warrant</td></tr>
<tr><td rowspan="2">2. Securing Scene</td><td>securing the crime scene</td><td rowspan="2">2. Identification</td><td>Identify seized items</td><td rowspan="2">2. Identification</td><td>Type of evidence</td></tr>
<tr><td>Evidence Preservation</td><td>Identify fragile evidence.</td><td>Evidence Storage location and format</td></tr>
<tr><td rowspan="2">3. Survey & Recogninationn</td><td rowspan="2"></td><td colspan="2" rowspan="2">3. Reconnaissance</td><td rowspan="2">3. Collection</td><td>Secure and preservation</td></tr>
<tr><td>Actual collection, storage and transportation</td></tr>
<tr><td rowspan="3">4. Documentation of Scene</td><td rowspan="3">Photographing, sketching and crime-scene mapping</td><td colspan="2" rowspan="3">4. Transport and Storage</td><td rowspan="3">4. Examination</td><td>Create image</td></tr>
<tr><td>Analyze evidence</td></tr>
<tr><td>Creating hash values</td></tr>
<tr><td colspan="2">5. Communication Shielding</td><td colspan="2">5. Analysis</td><td colspan="2">5. Reconstruction</td></tr>
</table>

<table>
<tr><td rowspan="2">6. Evidence Collection</td><td>Volatile Evidence Collection</td><td colspan="2" rowspan="2">6. Proof and Defense</td><td rowspan="6">6. Presentation</td><td rowspan="3">Documentation</td></tr>
<tr><td>Non-Volatile Evidence Collection</td></tr>
<tr><td rowspan="3">7. Preservation</td><td>Packaging</td><td colspan="2" rowspan="6">7. Archive Storage</td></tr>
<tr><td>Transportation</td></tr>
<tr><td>Storage</td><td rowspan="5">Sharing of findings</td></tr>
<tr><td>8. Examination</td><td></td></tr>
<tr><td>9. Analysis</td><td></td></tr>
<tr><td>10. Presentation</td><td></td></tr>
<tr><td>11. Result & Review</td><td></td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

Table 2:2 Comparison of the SDFIM, the DFMBMI frameworks to the WCDFIF Frameworks

2.9 Comparison of the SDFIM, the DFMBMI frameworks to the WCDFIF Frameworks

3.0 Survey on the application of Digital Forensic Frameworks: Phishing attack on a 5-star International Hotel

A 5-star International hotel chain suffered two cyber-attack in a span of eighteen months. Records for 5.2 million guests were compromised when hackers gained access to the hotels' database using the credentials of one of the employees at the reservation's desk. From its forensic analysis, the hotel estimated that the breach could have started in mid-January 2020 and detected the intrusion in late February. The attackers accessed an application providing services to guests in hotel establishments franchised under the hotel's brands through a phishing attack.

Systems affected by the attack included the personal identification information system and the loyalty app system. Data collected included contact details like guest names, home and email addresses, phone numbers and mailing addresses, personal details such as gender, birthday, name of employers, loyalty accounts information such as account numbers, loyalty points and partnership and affiliations such as frequent flier numbers, and finally preferences such as

language, hotel, and room preferences. The second attack was less severe compared to the first with data from the loyalty account such as passwords, card payment details, and passport information, and Identification cards not affected (Sundresan perl, 2021).

The researcher applied the SDFIM, the DFMBMI frameworks and the WCDFIF Frameworks to conduct an investigation and used the processes to evaluate the effectiveness of the frameworks.

Phishing attacks nowadays take many more forms than just email links and attachments. Now, social media feeds, search engines, browser extensions, pop-ups, chatbots, mobile apps, scareware, social engineering, and malvertising are all methods of phishing.

HTML phishing can bypass secure email gateways, next-generation antivirus endpoint security systems, and advanced endpoint protections by directly entering browsers and apps.URL inspections and domain reputation analyses can be completely evaded by these sneaky new attack vectors.

a) **Hardware and Software specifications of the computer**

The laptop computer used by the employee was surrendered to the authority and below are its specifications

Model	HP Laptop 15-dy5097nr
Operating System	Windows 10
Processor	Intel® Core™ i7-1255U (up to 4.7 GHz with Intel® Turbo Boost Technology, 12 MB L3 cache, 10 cores, 12 threads)[6,7]
Graphics	Integrated: Intel® Iris® Xᵉ Graphics
Memory	16 GB DDR4-3200 MHz RAM (2 x 8 GB)
SSD	256 GB PCIe® NVMe™ M.2 SSD

b) **Forensic tools used for the investigation**

Name of forensic tool	Description
Autopsy 4.10	Forensic tool used to retrieve and store evidence
Access Data FTK	A tool used to scan disks in search of information and restore deleted files

Access password recovery tool	Tool used to crack encrypted files
Quick Stego	Tool used to hide or unhide hidden information on an image
Open Stego	Tool used to hide or unhide hidden information on an image
FreeWordExcel	Tool used to crack encrypted excel or word file
Zip Password Unlocker	Tool used to crack an encrypted .zip file
Passware Kit Forensic	Tool to crack encrypted files
Wire Shark	A protocol analyzer used to monitor the network for any abnormalities during investigations
Sleuth Kit	
Advanced Archive Password Recovery	Tool used to crack an encrypted .zip file

c) **Investigation of the Phishing attack using the Systematic Digital Forensic Investigation Model (SDFIM)**

Stage 1: Preparation

Obtaining a search warrant from the relevant authority, which gives the forensic team permission to carry out the investigations, is the first step in the preparation stage. After this permission has been granted, the team holds preliminary meetings to plan the order in which they will carry out the process and delegate responsibilities.

Stage 2: Securing the scene

Here, the investigator locates the general location where the computer is situated and restricts access to this area.

Stage 3: Survey and recognition

Next, the investigator walks through the area and identifies the computer itself and other devices attached to it.

Stage 4: Documenting the scene

By taking a lot of pictures and videos of the crime scene and the physical evidence, the investigator records and preserves the scene. They can also make a sketch of the scene to capture as much information as possible.

Stage 5: Communication shielding

To prevent external interference that could alter the evidence, the investigator isolates the computer and blocks all communication options with it.

Stage 6: Evidence collection

At this stage, If the computer is running, the investigator conducts live forensics. Live acquisition of volatile evidence, which includes memory details, file time stamps, swap files, and registry keys, is carried out by the investigator using tools like FTK Imager. Because the volatile evidence contains extremely important evidence that would be lost if the computer were to be shut down, the investigator performs this step with extreme caution. Additionally, the investigator collects any other computer-attached devices, such as memory cards, flash drives, or hard drives

Stage 7: Preservation

Here, the investigator transports and stores the evidence in a secure location after transporting it safely in appropriate materials and labeling each component.

Stage 8: Examination

In the examination, stage includes receiving instructions, clarifying those instructions if they are unclear or ambiguous, risk analysis, and role and resource allocation.

Stage 9: Analysis

In this step, Investigators combine the fragments of data and draw conclusions from the evidence they find. However, a specific crime theory may require multiple iterations of investigation.

Stage 10: Presentation

The examiner typically completes a structured report on their findings at this point, addressing both the initial instructions and any subsequent instructions. Additionally, it would include any additional information that the examiner deems pertinent to the investigation.

Stage 11: Result and Review

A review of an investigation can begin at any of the above stages and be straightforward and quick. It might include a fundamental analysis of what went wrong, what went well, and how the lessons learned can be used in subsequent tests. Additionally, the instructing party ought to be contacted for feedback.

Stage 12. Data Acquisition and Identification

The investigator prepared an organized working environment and ensured that both physical and operational infrastructures was ready to be used and laid down a list of tools and applications to use. The investigator ensured the use of an antivirus to detect malicious programs and viruses, a firewall to prevent malicious programs from accessing the computer and used the wire shark tool which is a protocol analyzer used to monitor the network for any abnormalities during investigations. The investigator first created an image of the evidence according to (Gordon et al., n.d.). The image captured personal data of the computer user which included visited web pages and bookmarks, emails, cookies, encrypted files, operating system and user accounts. Later, the investigator used tools such as Autopsy and AccessData FTK to filter out the different types of data. Such tools will be easy to help filter out the present of encrypted files, check if there could be emails or communication between the attacker and suspected staff or if there are mismatched files present in the computer.

Stage 12. Verification tools

The hash value was created and verified by the investigator prior to the beginning of the evidence analysis. Since it checks the integrity of the evidence both during and after the analysis, the process of creating the hash value is crucial. To assist with this task, the investigator must generate a hash value following collection. The digital forensics examiner ought to generate several hash value and keep track of the data as it was initially collected. The

investigator can still demonstrate that the acquired evidence is identical to the original by comparing the image's hash values to those of the source. The investigator also used the utility tool for checksum either (MDA or SHA) to confirm the value's authenticity. This checksum is used to identify files uniquely, check for file integrity, and identify duplicate files.

Stage 13. Evidence data analysis

The investigator discovered hidden programs on the html files that were used to mine and store customer information like name, contact information, passport number, bank account information, and loyalty account information from the analyzed evidence. A suspicious video file was also found by the investigator. The investigator extracted the HTML file and gave it the name evi1.html by utilizing the Autopsy tool. The investigator also discovered a trail of suspicious email from the suspect's personal email in which his login credentials were shared, which allowed him to access the reservation and loyalty program systems of the hotel. The researcher named this in evi2.html after extracting it.The investigator also obtained a video file using the AccessData FTK tool that showed the suspect how to install a program that would use keystrokes to mine data and run simultaneously with reservation and loyalty program systems.

In addition, the investigator discovered that a Hiderman program was utilized as a steganography tool to encrypt a video file in order to conceal the video and conceal the intended actions. Based on the computer's web history, the user accessed various internet banking pages for various international banks, leading the investigator to believe that the suspect may have attempted to access multiple banks.

Stage 14. Reconstruction

The reconstruction phase was only present in the proposed WCDFIF. Here, the security guidelines and caution when handling the evidence were adhered to. Event reconstruction helps to prove or disprove a working hypothesis about a case. Event reconstruction amalgamated the results from the analysis and activities from prior stages and any other relevant information obtained during the investigation to recreate the crime scene.

The reconstruction of evidence helped the researcher clearly determine who was responsible for the information theft, with a probable time and chronology of how the theft happened. The

reconstruction was also able to prove that that particular computer was used to carry out the phishing attack. Event reconstruction was also able to point put the person, what they did and the systems and devices used.

Moreover, the reason why digital forensic analysis necessitates the creation of a theory to support event reconstruction methods is to improve analysis efficiency. The formalization of reconstruction techniques would make them simpler to automate, which could speed up their execution. Secondly, to make analysis more effective. Current reconstruction techniques' informal reasoning increases the likelihood of incorrect conclusions being drawn. The creation of a formal reconstruction procedure based on a well-established computer science theory would improve the analysis's efficiency. Reasoning errors would be less likely as a result of this. Lastly, to meet the admissibility requirements. The legal requirements for expert evidence's admissibility support the existence of a solid theory regarding the operation of reconstruction techniques.

Chain of Custody

The WCDFIF if adapted will ensure that an investigator maintain a proper chain of custody during all phases to preserve the integrity of the evidence and prevent it from contamination. Tampered evidence can change the state of the evidence increasing its chances of inadmissibility if the evidence is presented in court. The chain of custody helps indicate where the possible evidence might lie, its source, author, and the type of equipment the evidence interacted with. A weak or missing chain of custody may make a case lose its credibility in court.

The WCDFIF outlines the following steps to ensure the enforcement of a proper chain of custody. First, an investigator needs to save the original materials associated with the evidence. At all times, the investigator must create an image of the digital evidence, carefully store the original at a secure place and work from the copy. This way, one is able to compare the findings of the analysis during the reconstruction phase to the original that you preserved. Secondly, a researcher needs to take photos of the crime scene including images of the physical evidence before any collection or analysis is done. Thirdly, an investigator need to take screenshots of the evidence especially where the evidence is intangible. Next, the investigator needs to record the date, time, timestamps, or any information that will help create a chronology of where and

how the evidence was created and extracted. The fifth step is to systematically add a clone of digital evidence content into the forensic computers as this ensures that the researcher acquires a complete duplicate of the digital evidence in question. Lastly, an investigator need to carry out a hash test investigation to validate the image of the evidence being worked on. Performing a hash test ensures that the data we obtain from the previous copy is not corrupt and reflects the true nature of the original evidence failure which may indicate a flaw in the process and that the original evidence was tampered with.

Presentation

The results of the analysis were documented in a report that was clear and precise and demonstrated the findings and processes through the use of figures, graphs, and outputs of tools. The researcher also included supporting documents, such as the chain of custody and a detailed description of the procedures used and steps taken to scrutinize and extract data from the evidence presented. The researcher took into account the purpose of the investigation and used the documented finding to prove the objectives of the investigation. The report also included the limitation of the findings and the challenges encountered.

Second survey analysis case to be investigated

A new start-up SME (small-medium enterprise) with an E-government model based in Europe has begun to notice irregularities in its product and accounting records. It has carried out a preliminary check of the system log files and discovered a number of suspicious entries as well as IP addresses and a significant amount of data being transmitted outside the company firewall. They have also recently received a number of customer complaints stating that they are frequently redirected to a payment page that does not appear to be legitimate and that they are frequently presented with an odd message while their orders are being processed.

The company employs a general-purpose e-Business package (Ecommerce) and has a small team of six IT support specialists; however, they do not believe they have the expertise necessary to conduct a comprehensive malware/forensic investigation.

The company has hired a digital forensic investigator to find out if any malicious activity has taken place and to make sure that their systems do not contain any malware because of the increased competition in the high-tech industry.

Your job is to look into the team's suspicions and tell them how they might get rid of any malware-infected machines and make sure that no other machines on their premises or in the network have been infected. Additionally, the team wants you to conduct a digital forensics investigation to determine whether you can identify the root cause of the issues and, if so, to prepare a case against the culprits.

Windows Server NT is used by the business for its servers. The IT support team applies patches every month, but the team has noticed that some machines do not appear to have been patched.

Expected deliverables

This assignment requires you to submit a 5,000-word report outlining approach to the following issues:

a) Malware investigation.

b) Digital forensic investigation one should give a general overview of the approach taken and make a well-reasoned case for why the approach you chose is useful.

Additionally, one should talk about the steps and clear framework you will take to gather evidence and the necessary guidelines for digital evidence collection.

As part of the report, one should also give a critical evaluation of the tools and techniques that are currently used for digital forensics or malware investigations and how effective they are. You should talk about things like the consistency of the approaches taken, the skills that forensic investigators need, and problems with existing methodologies (especially in light of the fact that there isn't a single common global approach to carrying out such investigations and the issues that can arise when an investigation needs to be carried out across international boundaries).

Overview analysis of above survey

The following are the forensic investigations' scopes for this particular case:

to determine the malicious activities in relation to the 5Ws (Why, When, Where, What, and Who); to determine the security flaw in their network; to determine the impact, if the network

system was compromised; to determine the necessary legal procedures; to provide the corrective action necessary to harden the system.

The investigation's legal difficulties, according to Rahim and Ekbatanifard (Pourvahab & Ekbatanifard, 2019, 2019; Rahim et al., n.d.-b), the following legal obstacles must be overcome before we can begin our forensic investigation:

a) Getting written permission to conduct the forensic investigation, unless another incident response authorization procedure is present

b) Discussing with the legal advisors to identify the potential issues that can be raised during the improper handling of the investigations.

c) Ensuring that the clients' confidential and privacy issues are taken into account

Initial preparation

Initial preparation it goes without saying that in order to carry out the investigation in an effective manner, we need to make preparations before we begin. According to Rahim (Rahim et al., n.d.-b)this is regarded as an investigational proactive step. During the stage of preparation, the following actions must be taken:

a. Collecting all information from the incident assessment, including information about the incident's severity.
b. Determining how the investigation will affect the SME business in terms of downtime for the network, recovery time from the incident, revenue loss, and confidential information loss.
c. Getting information about networks and network devices like routers, switches, hubs, and so on, a network diagram, computers, servers, and topology documentation
d. Identifying external storage devices like memory cards, CDs, DVDs, pen drives, external hard drives, and remote computers.
e. Figuring out which forensic instruments can be used in this investigation.
f. Using "netmon" tools to capture live network traffic in the event that the suspicious activities are still going on.
g. Keeping track of everything that happened during the investigation so that it can be proven in court that the plan of action was followed.

• To ensure the integrity of the data, imaging the hard drive of the target devices and hashing it with MD5

Collection

The first step in the collection process is to identify, label, record, and acquire data from potential relevant data sources while adhering to data integrity-preserving guidelines and procedures. In the course of a computer forensics investigation, there are two distinct categories of data that can be gathered. There are two types of data: persistent data and volatile data. Random Access Memory (RAM), the registry, and caches are examples of volatile data that are present when the system is powered on but are erased when it is turned off. On-volatile data, such as HD documents, are stored on a system even if the power is off. A computer forensic investigator must be aware of the best way to capture volatile data because it only lasts a short time. Local or remote collection of evidence is possible.

Volatile data the method for capturing volatile data is depicted in the figure below. The target machine, in this case the Windows NT Server, must be in the same LAN as the forensic workstation. The forensic workstation's Cryptcat tools can listen to the Windows NT server's port. Open the trusted console cmd.exe and execute the following command to create the optical drive for the trusted toolset on the Windows NT server:

To capture the data at the forensic workstation, we use the following command:

cryptcat -l -p 6543 -k key >> <file name>

Figure 12.3 Volatile data collection setup

Source :(Flandrin et al., 2014)

Finally, in a computer forensic investigation, collecting clipboard content is also crucial. If the anomalies in the SME are still present, we can retrieve a lot of important evidence from the running processes, the network connection, and the memory-stored data from a machine that is still running (Flandrin et al., 2014). When the machine is in the volatile state, there is a lot of evidence; therefore, in order to collect such evidence, it must be ensured that the affected computers are not shut down.

None- volatile data

After the volatile data have been captured, the non-volatile data are examined. Copying the content of the target system as a whole is the first step in non-volatile data collection. Another name for this is "forensic imaging. With imaging, the original data can be preserved as evidence in the event of a malfunction or data change during the forensic investigation. Forensic tools like EnCase, ProDiscover, and FTK will be used to create forensic imaging. To connect to the target system and copy the entire contents of the target drive to another storage device without using any of those forensic tools, a forensic investigator employs a write blocker. The only goal of hard drive cloning is to duplicate the entire system. The raw image that is created during hard drive cloning will be copied in its entirety; no additional content will be added. The metadata in forensic imaging, for example, compresses all empty blocks using hashes and timestamps.

In both offline and online investigations, data collection is possible. Offline research is an option for forensic imaging. Using tools like ethereal or Wireshark, online investigation can look at live network traffic. Under non-volatile data collection, the investigation will collect firewall, antivirus, and domain controller logs. We will also collect application logs, IDS logs, database logs, Windows event logs, and Web server logs. All digital evidences must be recorded in the custody log chain after they have been collected. The purpose of the chain of custody log documentation is to preserve the integrity of the evidence from the beginning to the end of the investigation, up until the presentation of this investigation report(Pourvahab & Ekbatanifard, 2019).

We need to image the disk bit by bit before starting any other processes. This will allow us to access the entire volume and copy the original media, including the deleted files. We should hash everything after the disk has been imaged to guarantee the data's authenticity and maintain its integrity throughout the investigation. We must ensure that we do not alter the data from the

time we collect it until the end of the investigation, and the hash values must be recorded in multiple locations. For the digital forensic investigation in this case, target system hard drives, external storage devices, and the Windows NT Server hard drive must be acquired (Flandrin et al., 2014).

Examination

The examination will be performed in the following areas, examine the file system, Windows registry, Network and Database forensic examination, as follows:

NTFS Disk is a file, and NTFS is the New Technology File System. The Master File Table (MFT) is the first file in NTFS and contains information about all files and disks. Metadata is another name for the records in the MFT. There are two ways files can be stored in MFT:non-residents and residents . In the MFT, files smaller than 512 bytes can be stored as resident files, while files larger than 512 bytes can be stored outside the MFT as non-resident files. In Windows NT, when a file is deleted, the operating system will rename it and move it to the Recycle bin with a unique name. The info2 file is where the operating system stores information about the original file name and path. However, associated clusters are marked as available for new data if a file is deleted from the recycle bin.Because it recovers deleted space faster than FAT, NTFS is more effective. Because NTFS disks are data streams, they can be added to an existing file. These are some ways to store a data stream file:

C:echo text_mess > file1.txt:file2.txt

Windows registry examination

Examining the Windows registry According to (Rahim et al., n.d.-b), a registry can be considered a log file because it contains data that can be retrieved by a forensic investigator. The associated key values are referred to as the "Lastwrite" time, which is stored as a FILETIME and is regarded as the file's last modification time.The Lastwrite indicates when the registry was last modified, whereas it is frequently challenging to determine the precise date and time of file modification.Fantastic will go over a few specific steps (Rahim et al., n.d.-b)for analyzing the organization's windows registry to make sure the problems inside and outside the company are known and being fixed to keep the company's reputation safe.

The Windows registry is a set of databases that Microsoft used in Windows 98, Windows CE, Windows NT, and Windows 2000 to store a user's or user application's configuration as well as the configuration of hardware devices. This information is used as a reference point when a program or processes are run (Windows, 2013).

Network analysis forensics

Network forensics is the process of acquiring, collecting, and analyzing events that take place in the network. It can also be referred to as packet forensics or packet mining at times. The fundamental goal of network forensics is the same: to gather information about packets in network traffic like emails, queries, and web content browsing.

The process of acquiring, collecting, and analyzing network-related events is known as network forensics. Sometimes, it is also referred to as packet forensics or packet mining. The primary objective is to collect data about packets in network traffic like emails, queries, and web content.

Database forensics analysis

A database is a collection of files or files representing a collection of data or information. Using a set of queries, the data can be retrieved from the database. The use of computer investigation and analysis methods to extract evidence from a database and present it in court is referred to as database forensics. The identification, preservation, and evaluation of data are the primary focuses of database forensics. Users must obtain authorization and authentication from the database servers in order to access the database, as stated by (Pourvahab & Ekbatanifard, 2019).After authorization has been completed, only the user can access the data and, if desired, alter the data. A list of the users who were granted access to the data can now be found by looking through the audit logs of the database. Because there is a possibility that the data could be altered by either an authorized user or an unauthorized user, the team needs to look up the IP addresses of the remote connections in the database.

Analysis

They must examine and evaluate the evidence that was gathered. Investigate the data to determine whether any unusual or hidden files are present. Then, check to see if any unusual processes are running and if any unusual sockets have been opened. Also investigate any

unusual application requests. Then, check the account to see if there are any unusual ones. The patching level system, whether it has been updated or not, will also be discovered. Learn whether any malicious activities are presented based on the results of those analyses. Then, come up with a new plan for the forensic investigation that includes things like complete memory and file system analysis, event correlation, and timeline analysis (Pourvahab & Ekbatanifard, 2019).Our initial analysis also confirms that there are malicious activities in their network system, as revealed by this case survey.We need to conduct malware executable analysis in order to determine the capabilities and goal of the malicious code.There are two types of malware executable analysis: static analysis and behavioral analysis.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

Methodology demonstrates how the researcher collected data and all the information required to completing the study entirely. This work's primary aim was to assess the application of digital forensic frameworks with a focus in Kenya, and evaluates how the CA conducts cybercrime investigations. Additionally, the study analyzed the effects of the available forensic tools, investigators' capabilities and the existing laws and regulations and laws in investing crimes. The research methodology section, sample size, sampling procedure, target population, data collection methods, study tools, data analysis and processing, instrument reliability and validity, and ethical and legal concerns are examined in this chapter.

3.2 Research Design

Information technology is social science were by both experimental and descriptive survey design can be efficiently be combined.in this study the design was quasi experimental and descriptive design. Both the respondents were required to have interacted with different systems of frameworks in this case we were target to give their feedback depending on observation and experiences .it quasi experimental because the was not controlled environment. The research design adopted both quantitate and qualitative approaches.

A quantitative approach was used in this study where numeric analysis was required for the correlation question relating to which requirements were needed to developing the new digital forensic investigation framework According to (Mugenda and Mugenda, 1999, p.160) a survey research design is a process of collecting data for testing hypothesis or to answer questions regarding the current status of the subjects in the study. The researcher built hypothesis based on the set variables, designed the experimental treatments and finally tested the validity and reliability of the results.

The research design contains the carefully chosen plan followed in the collection of data. The design assisted with managing the data collected and helped in the formulation specific information relevant for review. This Information was collected through the use of questionnaires and interviewing key respondent.

3.3 Research Site

The study was conducted at the Communication Authority of Kenya. The CA is the regulatory authority for all the actors within the Information Communication and Technology sector. Additionally, the CA has a Computer Forensic lab that deals with both dynamic and static data.

3.4 Target Population

This study targeted 105 individuals working at the Computer Forensic lab at the CA.

3.5 Sampling procedures and Sampling size

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

3.5.1 Sampling Procedure

A sample

The procedure used in sampling the respondents was both stratified, simple random, purposive techningues due to the fact that the study population was heterogeneous. This sampling technique targeted a particular group and consisted of individuals, objects, and events with the same observable characteristics (Etikan, 2016). This study-targeted a population of 35 individuals working within the Cyber Security department at the CA because they are knowledgeable and have experience in application of forensic science in cybercrime investigations. Table 5 shows the total number of respondents targeted in the study.

Designation	**Population(N_i)**	**Proportion (N_i / N)**	**Sample (s_i)**
Director Cyber Forensics Lab	1	0.01	1
Deputy Directors Cyber Forensics Lab	4	0.04	2
Cybersecurity Incident Responders	26	0.25	8
Cyber Security & Tech Specialists	19	0.18	6

ICT Policy & Regulation officers	21	0.20	5
ICT Data Analysts	18	0.17	3
Cyber Investigations & Forensics Officers	16	0.15	9
Total	**105**	**1.0**	**35**

Table 3:1 Number of targeted respondents

Source: Researcher

3.5.2 Sample size

Sample sizes are important while conducting a research since they represent a portion of the target population (Hamed Taherdoost, 2017). The outcome of the research is affected by the sample size and a size of 10%-30% of the targeted population gives reliable results (Mugenda & Mugenda, 2003). As a rule of thumb, a sample of 10% is sufficient to represent the entire population (Blanche et al., 2008). The researcher sampled 35 respondents (33.3%) to represent t the target population of 105 staff working at the lab, this percent is higher than recommended to account to for non-responsive respondents if any.

3.6 Data Collection

The researcher used questionnaires and scheduled interviews to collect data from the respondents. Physical data collection was limited due to the current COVID-19 pandemic and therefore most of the information was collected online through google forms.

3.6.1 Research Instruments

The researcher proposed to collect primary data through Google form questionnaires and key informant interviews questions for the director and deputy directors of the lab. Questionnaires were designed for officers from the Cybersecurity, ICT Policy & Regulation, Data Analysis, and the Investigations and Forensics departments of the lab. The research was grouped into two sections namely the background information and the research questions. Questions in the questionnaire and interview were coined around the research questions, using a mixture of both structured and unstructured formats to aid in the collection of as much information as possible.

The questionnaire yielded in checking its validity by using statically tools like SPSS it ensure is best suited during pilot testing

3.6.2 Pilot Testing of Research Instruments

The pilot study was conducted at the Directorate of Criminal investigations (DCI) forensics investigations lab to establish the validity and reliability of the research instruments. The instruments were administered to 10 officers at Directorate of Criminal investigations randomly

Five (15.6%) random respondents were used during the piloting to confirm the reliability of the research instrument.

3.6.3 Instrument Validity

Validity in research shows the degree to which the results truly measure what they were supposed to measure (Cohen et al., 2009). Validity was assessed by examining how well the results agree to established concepts and other variables of the same idea. Valid tests are reliable only when they produce accurate results that are reproducible. The pilot conducted to check the validity helped in the identification of ambiguous questions in the proposed questionnaire and this further aided in mapping out the relevant questionnaire useful for the deduction of desired and accurate results. For this research, the instruments were discussed by digital forensics examiner at DCI digital forensics lab and colleagues of Kenya Colllege of Accountacy (KCA)masters class to ensure questions were clear and unambiguous both in terms of language, content and implied meaning before being rolled out for data collection.

The researcher used the content validity approach to collect the data. The content validity approach refers to the ability of an investigation to capture all aspects of the intended field (Taherdoost, 2016).

3.6.4 Instrument Reliability

Reliability is a measure of the extent of consistency of study results and if the same results can be achieved when the research is repeated under the same conditions. (Taherdoost, 2016). The researcher applied the internal consistency method to determining the reliability of the research instrument. For this case, the researcher piloted 10 questionnaire instruments at DCI cyber

security depart and then applied Cronbach's alpha coefficient to measure the questionnaire's internal consistency.

3.7 Data Analysis

The data collected was cleaned, tabulated and grouped to meaningful patters and themes with a view to summarizing the findings.

A different approach was used to analyze both qualitative and quantitative data. Qualitative analysis entails categorizing, tabulating and assembling evidences to address the research questions. Further, the data was grouped into meaningful patterns and themes that helped in the summarizing and organization of the data. Statistical Package for Social Sciences (SPSS) was used for descriptive and quantitative analysis. From this, quantitative data was presented inform central tendencies, frequencies, graphs, charts, and tables.

Developed framework for digital forensics investigations

A formal process framework is needed to allow digital forensics practitioners to adopt a consistent approach and to enable courts to determine the reliability of digital evidence presented to them This framework should also be general, as it can be applied to all areas of digital forensics, including law enforcement, business, and incident response. No such integrated process framework, both formal and general, currently exists. To address these shortcomings, this article proposes a formal framework that allows digital forensics practitioners to adopt a clear and consistent approach to digital forensics and investigation, which is universal in that it can be applied in a variety of settings where digital forensics can be used. The table illustrate the stages and sub stages of the proposed framework

Wycliffe Comprehensive Digital Forensic Investigation Framework (WCDFIF)	
Stage	**Sub-Stage**
1. Planning	Understand and document reason for investigation
	Obtain search warrant
2. Identification	Type of evidence
	Evidence Storage location and format
3. Collection	Secure and preservation
	Actual collection, storage and transportation
4. Examination	Create image
	Analyze evidence

	Creating hash values
5. Reconstruction	
6. Presentation	Documentation
	Sharing of findings

Source: Researcher

CHAPTER FOUR
DATA ANALYSIS AND PRESENTATION

4.1. Introduction

This chapter presents the data that was collected on the effectiveness of using digital forensics frameworks within CA in combating cybercrime in Kenya. A sample of 35 people participated in the study, and questionnaires were given to each one. An examination of the personal information of the participant's kicks off the chapter, and then looks into the analysis of the nature of training in digital forensic science and how they relate to investigations, technology, the legal framework and regulatory policies that make up forensic digital evidence, the forensic procedure, and the adaptability of digital forensics are all important aspects.

4.2. Questionnaire Return Rate

Out of the sampled population, 29 questionnaires were filled in making a response rate of 82.9%. The response rate was representative and was adequately used to answer the research questions.

Response	**Frequency**	**Percentage**
Filled in questionnaires	29	82.9 %
Un returned questionnaires	6	17.1 %
Total Response Rate	**35**	**100**

Table 4:1 Response Rate

Source: Researcher

4.3.0 Demographic Characteristics of Research Respondents

The participant's personal information included: gender, age, the highest level of educational qualification, and the period of time the participants have been involved in the digital forensic investigation in Kenya.

4.3.1 Participants Gender

The participants were requested to indicate their gender in order to inform the researcher as to whether gender is a factor in determining the conduction of forensic investigations. 22 out of the 29 participants who responded to the study were male at 75.9% 7 were female representing

24.1%. This depicts that male was mostly involved in the conduction of digital forensic investigations.

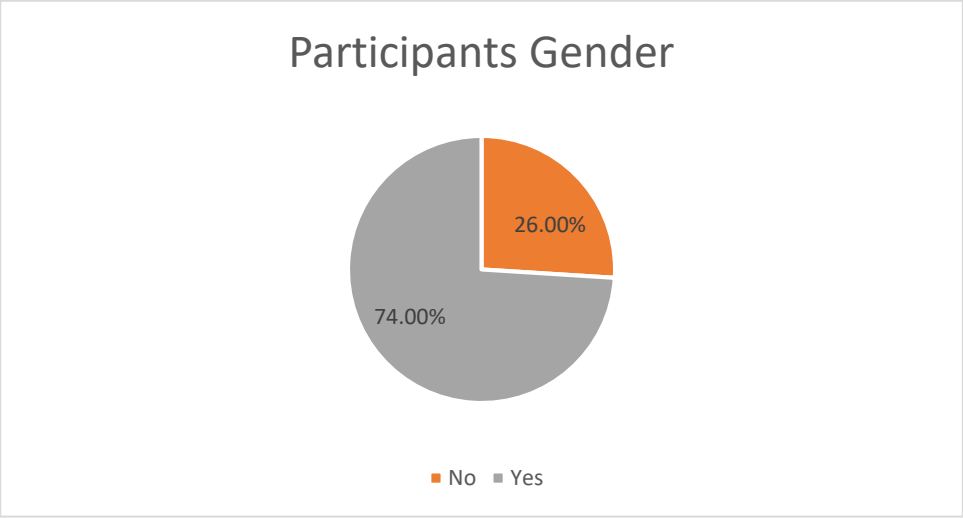


Figure 4:1 Participants Gender
Source: Researcher

4.4 Distribution of Participants by Level of Education

The participants were requested to indicate their level of education.

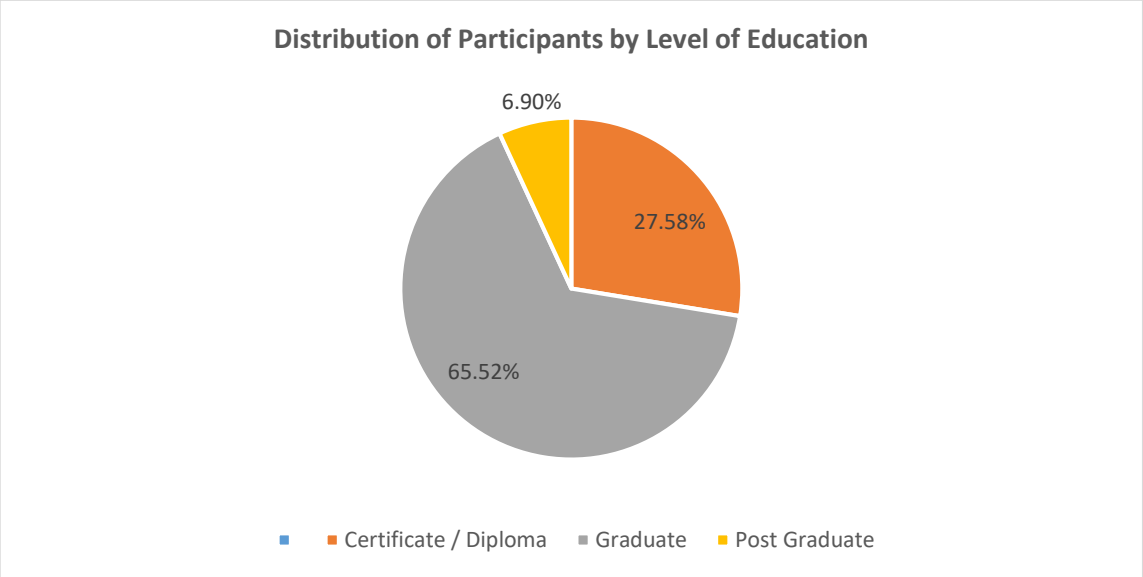


Figure 4:2 Distribution of Participants by Academic Qualification
Source: Researcher

From the findings, most of the participants (65.25%) had a graduate level of education. This implies that participants had ample knowledge on digital forensic investigations and hence higher chances of getting reliable data. This was significant because it allowed the researcher to determine whether the participants were actually aware of what forensic investigations entailed and whether the provided information was accurate.

4.5 Work Experience in Forensic Investigations

The study also sought to establish the extent to which participants had being involved in Digital Forensic Investigation.

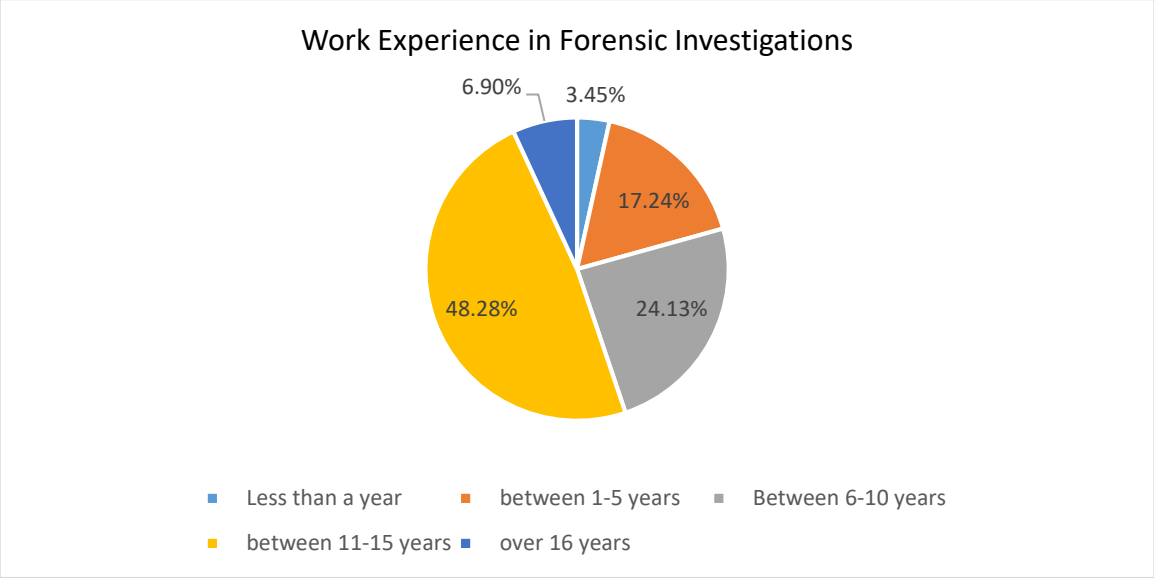


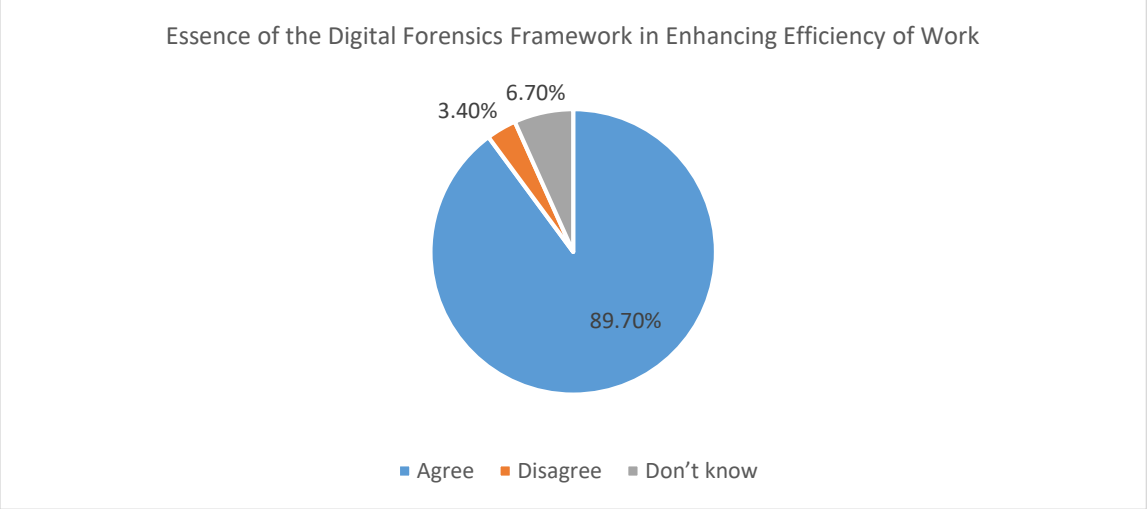
Figure 4:3 Duration of being involved in field of digital forensics investigations
Source: Researcher

Based on the findings most of the research participants (48.28%) have been involved in digital forensic investigation for a duration between 10 - 15 years with only 2 having over 16 years' experience. Subsequently, this illustrates that most of the officers had been involved in forensic investigations for a longer duration and thus could offer concrete information.

4.7.2 Essence of the Digital Forensics Framework in Enhancing Efficiency of Work

The participants were requested to explain the essence of using the digital forensics framework in enhancing the efficiency of work and 89.7% indicated that frameworks gives guidelines on the processes and procedures suitable in handling different pieces of evidence. Important to

note that framework also encourage proper chain of custody meaning that the integrity of evidence will always be maintained, giving it higher chances of admissibility in court.



Adopting a clear chain of custody when performing digital forensic investigations

The participants were asked to indicated whether a adopting a clear chain of custody when performing digital forensic investigations improves the investigation process

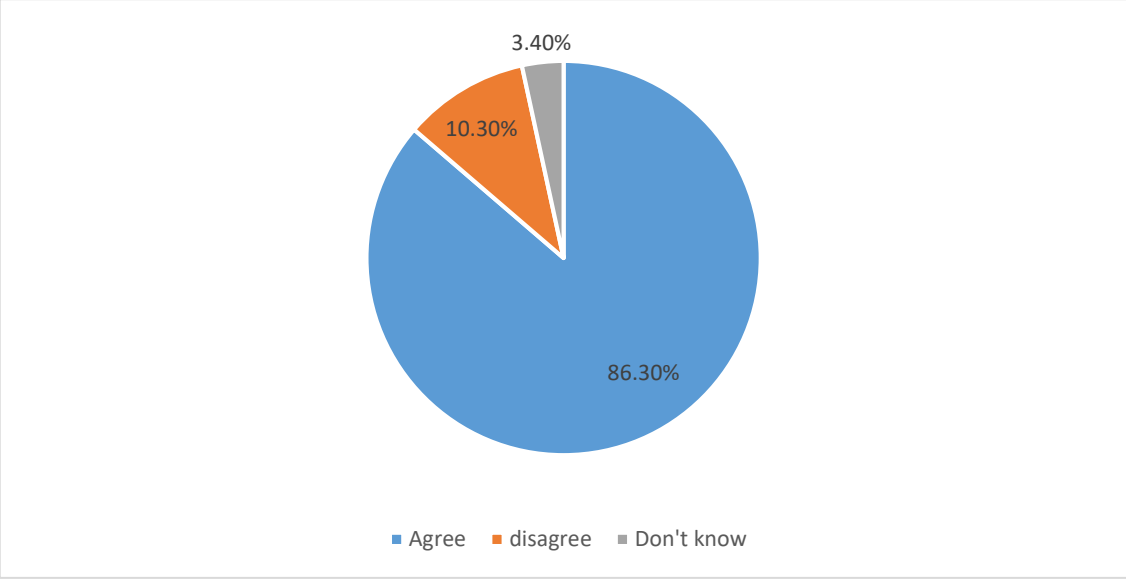
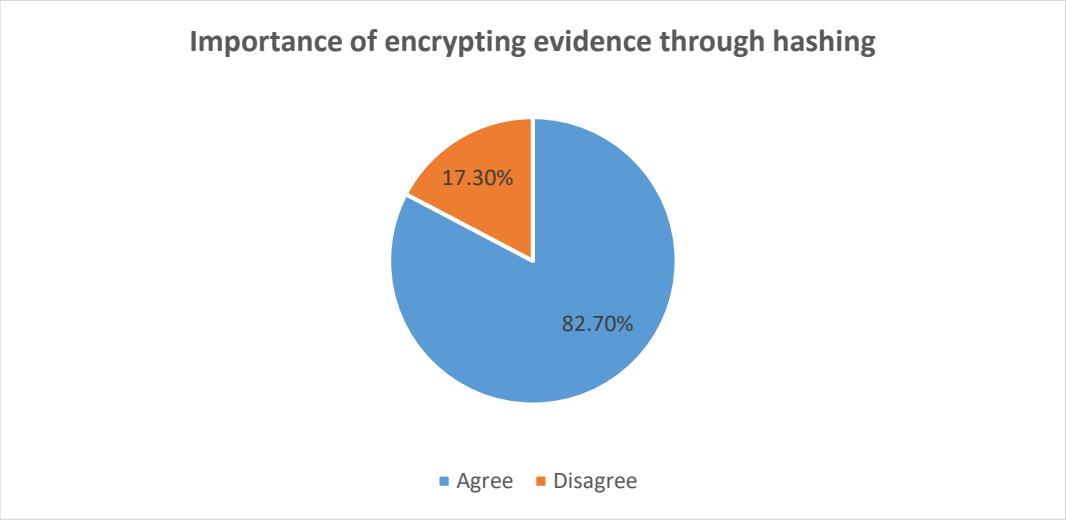


Figure 4:5 ***adopting a clear chain of custody when performing digital forensic investigations***

As shown in figure 4.5 above, majority of the respondents, 86.3%, agreed that adopting a clear chain of custody when performing digital forensic investigations is the most important task in computer forensics. 10.3 % of the respondents disagreed that adopting a clear chain of custody when performing digital forensic investigations is the most important task in computer forensics, while 3.4% of the respondents didn't know that adopting a clear chain of custody when performing digital forensic investigations is the most important task in computer forensics.

Importance of encrypting evidence through hashing

The participants were asked to indicate the importance encrypting evidence through hashing in digital forensics investigations.

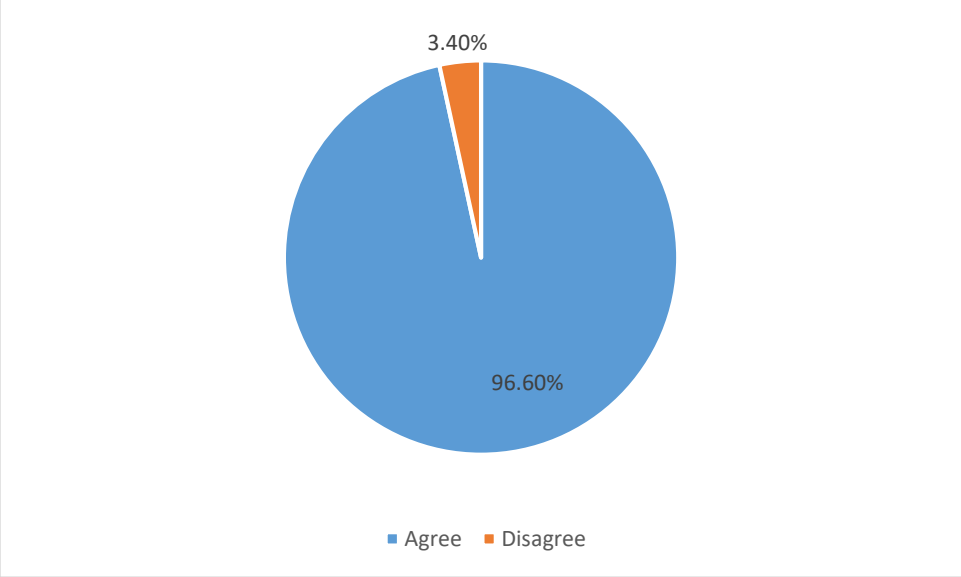


From the findings, most of the participants 93.1% agreed that encrypting evidence through hashing is key in the computer forensics investigation process. 6.9 % of the respondents encrypting evidence through hashing is key when performing digital forensic investigations is the most important task in computer forensics.

Re-construction of the crime scene to test investigative hypotheses and improve the integrity of the evidence.

Through the analysis of the crime scene pattern, the location and position of the physical evidence collected, and the laboratory examination of the physical evidence, crime scene reconstruction is the process of determining or eliminating the events and actions that occurred

at the crime scene. The participants were asked to indicate whether that process was important in digital forensics investigations process.



As shown in figure 4.5 above, majority of the respondents, 96.6%, agreed that reconstruction of the crime scene to test investigative hypotheses and improve the integrity of the evidence when performing digital forensic investigations is an important task in computer forensics. 3.4 % of the respondents disagreed that reconstruction of the crime scene to test investigative hypotheses and improve the integrity of the evidence is an important task in computer forensics.

4.13 Digital forensics framework for handling evidence according to work experience

The participants were requested to indicate whether they were fully certified with the framework they choose

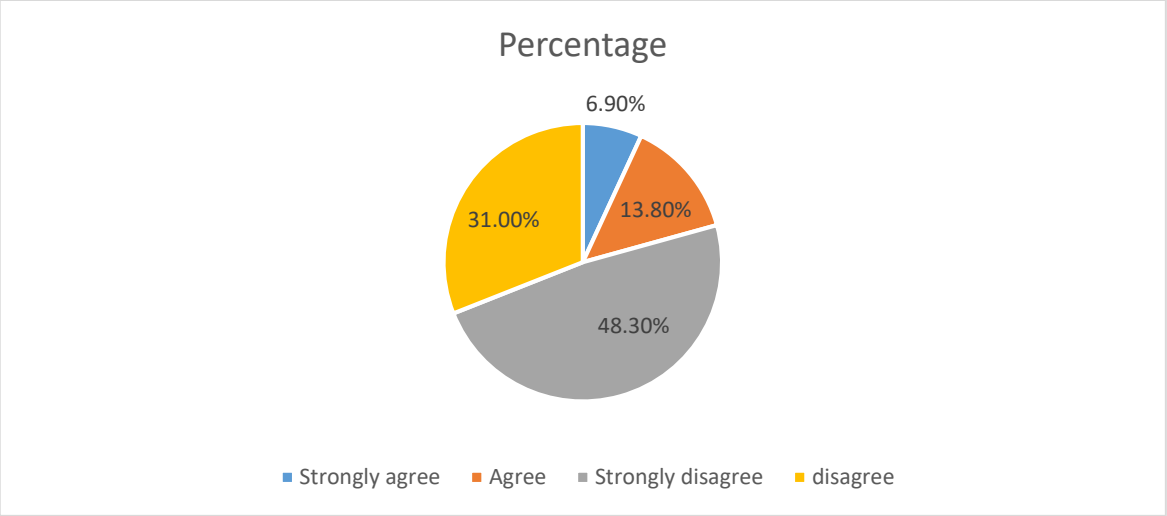


Figure 4.3 certified digital forensics framework

Source: Researcher

As shown in figure 4.3 above, majority of the respondents, 48.3%, strongly disagreed that they were not certified with the digital frameworks in place. 31.0 % of the respondents disagreed that that the frameworks in place were not full certifying their investigation process, while 13.8% of the respondents were indifferent opinion that the frameworks were good enough. On the other hand, only 6.9% of respondents strongly agreed that the digital forensics frameworks were good enough in handling any digital evidence processes.

4.9 Absence of Standard Digital Forensics Framework for Investigations

The participants were asked to indicate whether the absence of a standard digital forensics framework for investigations would have an influence on the reliability to produce concrete evidence. Figure 4.3 Absence of Standard Digital Forensics Framework for Investigations

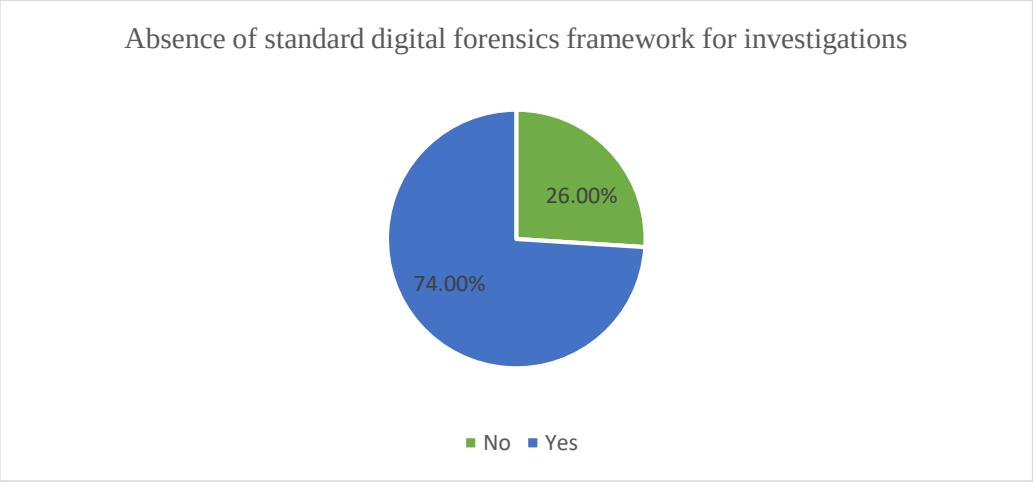


Figure 4:3 Absence of Standard Digital Forensics Framework for Investigations
Source: Researcher

From the findings majority (79%) of the participants indicated that lack standard of digital forensics framework have an influence on the reliability to produce concrete evidence while 21% indicated that absence have no effect. This depicts that absence of standard digital forensics framework have an influence on the reliability to produce concrete evidence.

4.10 Documentation and Reporting of results of forensics investigation

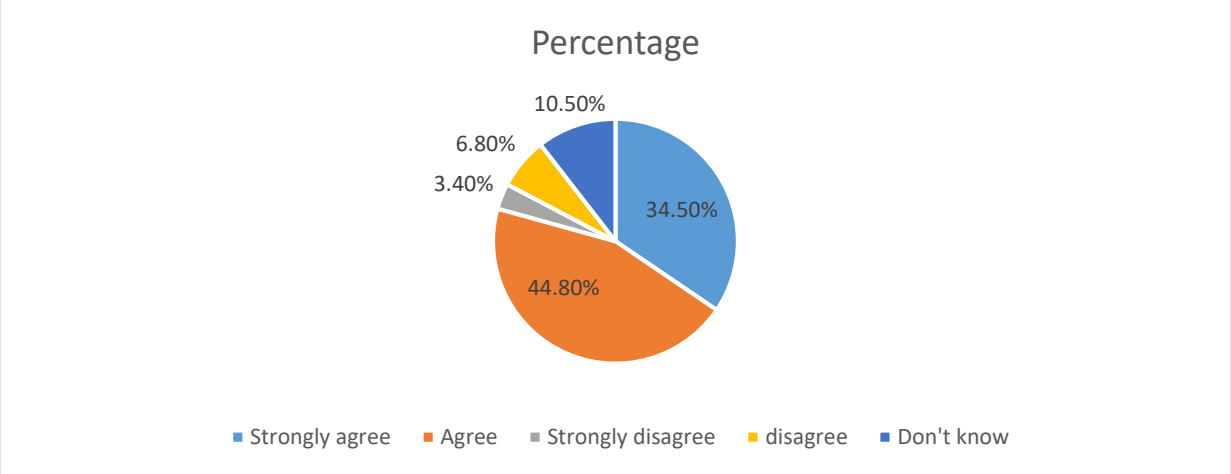


Figure 4:5 Documentation is the most important task in computer forensic investigation
Source: Researcher

The participants were asked to indicated the importance documentation, results and reporting in digital forensics investigations.

The majority of participants, 44.8%, agreed that documenting and reporting results is the most important task in computer forensics, as shown in figure 4.1.6 above. Documentation and reporting is viewed as the most important aspect of computer forensics by 34.5 percent of those polled, while 10.5% of those polled remained unconcerned about the topic.On the other hand, only 6.8% of respondents strongly disagreed that documentation and reporting is the most important task in computer forensics, and only 3.4% of participants strongly disagreed.

4.11 Standard Procedures and Policies for Conducting Forensic Investigations

The participants were requested to indicate whether there are standard procedures and policies for conducting forensic investigations in Kenya.

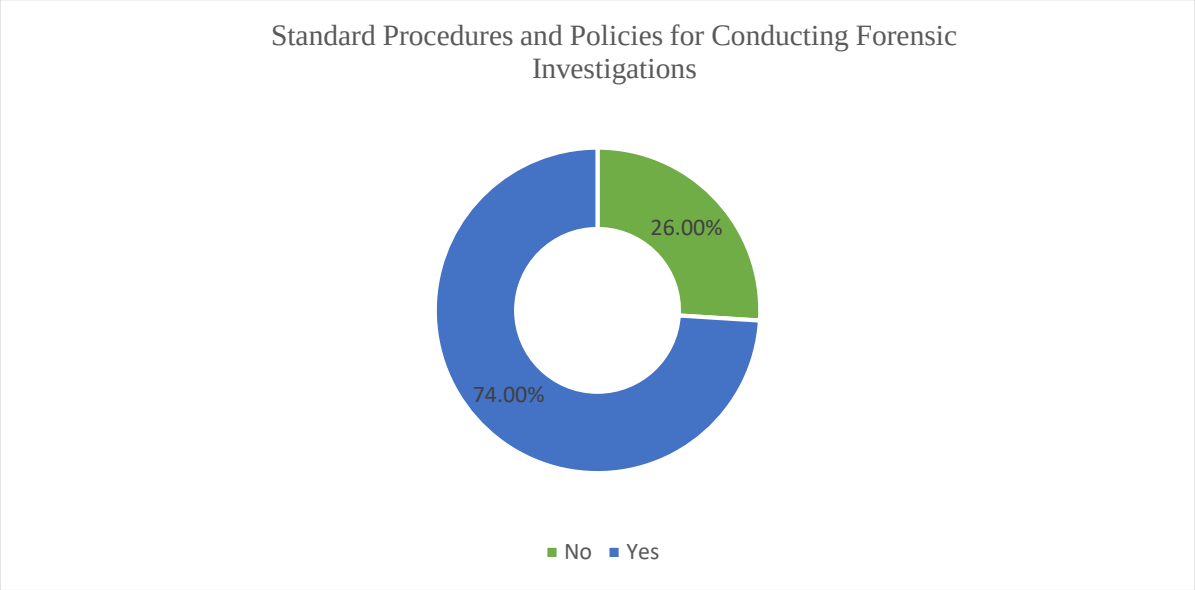


Figure 4:4 Standard Procedures and Policies for Conducting Forensic Investigations
Source: Researcher

Following standard procedures and policies while conducting forensic investigations in affects the quality of evidence produced. From the findings majority of the participants (74%) indicated that there were standard procedures and policies for conducting forensic investigations in Kenya while 26% indicated the absence of standard procedures. Applying the set rules that investigators follow ensures that evidence is not interfered with, is packed, and submitted to the departmental committee. In addition, the participants indicated that for analysis, the information is reconstructed and a case is formulated which help in aligning the suspect in Kenya.

4.17 Challenges Faced by Digital Forensic Investigator framework

The participants were requested to indicate the challenges faced by digital forensic investigators frameworks during the conduction of forensic investigations.

	Frequency	**Percentage**
Collection of evidence	1	3.4%
Creating hash values	10	34.5%
Time taken processing a case	5	17.2%
Reconstruction of Evidence	13	44.8%
Total	**29**	**100.0%**

Table 4:2 Challenges Faced by Digital Forensic Investigator framework
Source: Researcher

According to the participants the challenges included interference with the collection of evidence, creating hash values, Archive Storage, Time taken processing a case and reconstruction of evidence. 44.8% of the respondents strongly agreed on Reconstruction of Evidence is a big challenge, 34.5 % agreed that Creating hash values is a challenge in investigations, while 17.2% were indifferent opinion time taken to process a case is a challenge. On the other hand, 3.4 % of the respondents agreed that collection of evidence is a challenge.

Following the forensic investigation framework's guidelines speed up the investigation process and give more accurate findings.

The participants were requested to indicate whether following a forensic investigation framework's guidelines speeds up the investigation process and gives more accurate findings

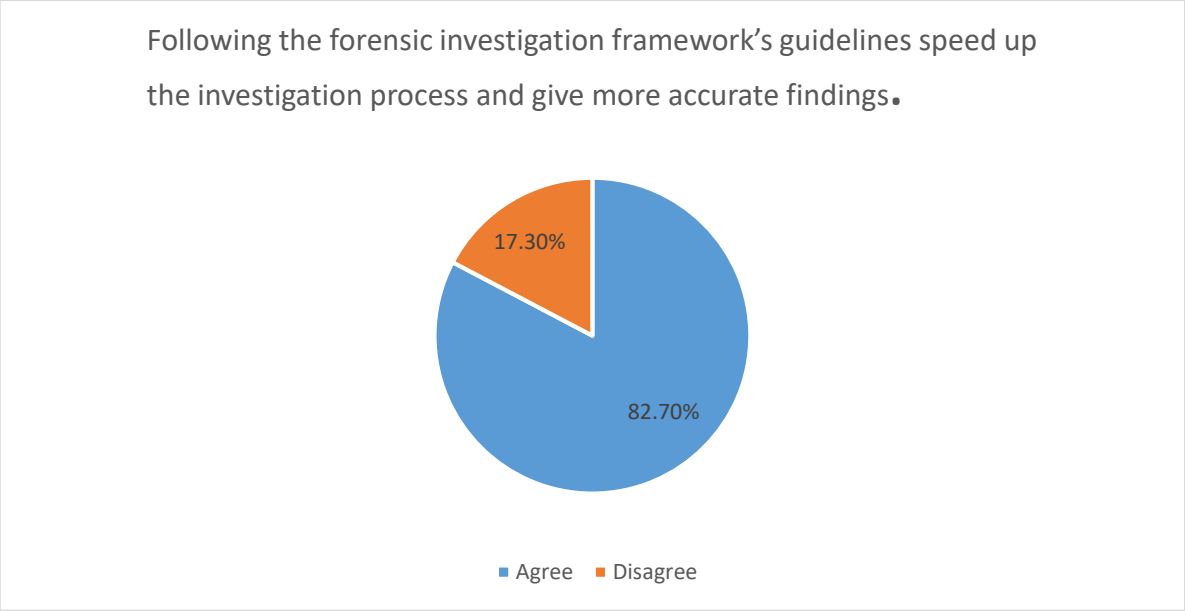


Chart
Source: Researcher

As shown in chart above, majority of the respondents, 82.7%, agreed that following a forensic investigation framework's guidelines speeds up the investigation process and gives more accurate findings while 17.3 % of the respondents disagreed that following a forensic investigation framework's guidelines speeds up the investigation process and gives more accurate findings.

4.12 Digital Forensics and Investigations Frameworks and their Reliability to Produce Concrete Evidence

This section presents findings on different digital forensics frameworks and their reliability to produce concrete evidence. The participants were asked to choose the preferred digital framework they would use when handling the digital forensics investigations process for reliability to produce concrete evidence. This was based on the survey analysis on page 22.

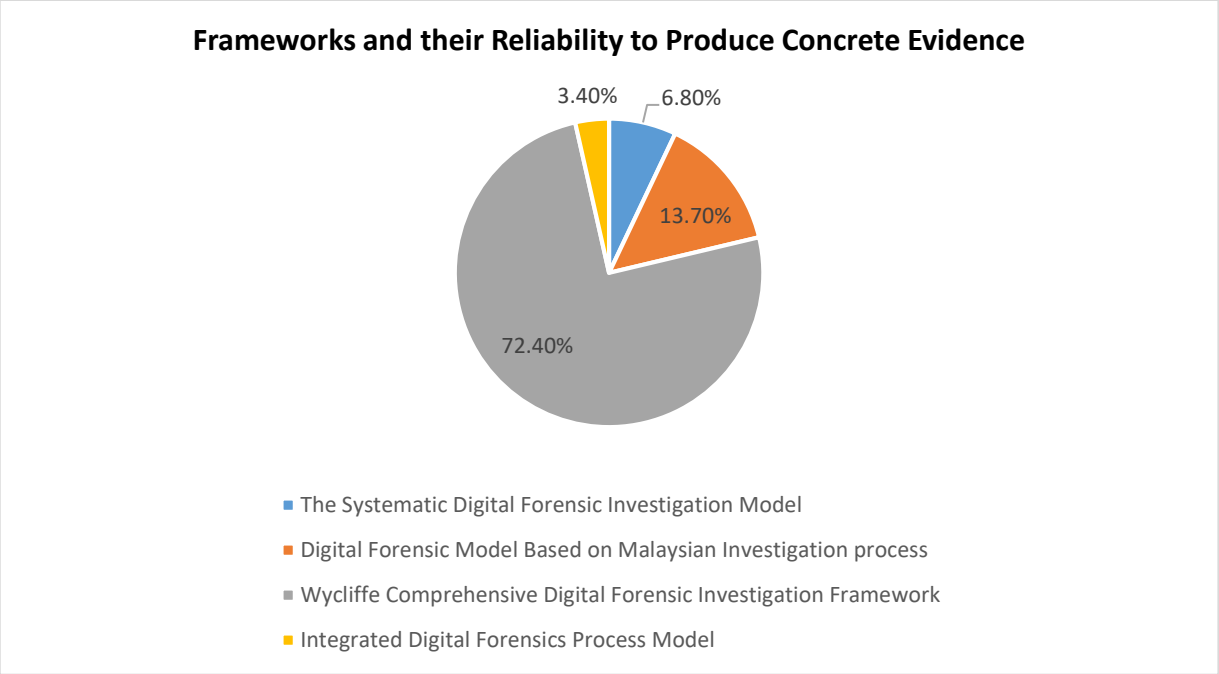


Figure 4.2 Frameworks and their Reliability to Produce Concrete Evidence

Source: Researcher

As shown in figure 4.2 above, majority of the respondents, 72.4%, selected Wycliffe Comprehensive Digital Forensic Investigation Framework would be the most suitable in reliable to produce concrete evidence in digital investigation process. 13.7 % of the respondents selected Digital Forensic Model Based on Malaysian Investigation process, while 6.8 % of the respondents preferred The Systematic Digital Forensic Investigation framework is the best in digital forensics investigations. On the other hand, 3.4% of the respondents selected Integrated Digital Forensics Process framework.

In a scale of 1-5, how efficient, reliable. Accurate and comprehensive the following frameworks when conducting digital forensics investigations. 1 Being the lowest (poorest) and five being the best.

Framework	scale	
The Systematic Digital Forensic Investigation Model	1	1
Digital Forensic Model Based on Malaysian Investigation process	2	1

Wycliffe Comprehensive Digital Forensic Investigation Framework	5	26
Integrated Digital Forensics Process Model	3	1
Total		**29**

Table

Source

As shown in table 4.2 above, majority of the respondents 26 in number selected Wycliffe Comprehensive Digital Forensic Investigation Framework would be the most efficient, reliable. Accurate and comprehensive the following frameworks when conducting digital forensics investigations, while other framework where selected by one respondents

4.20 Conclusion

In conclusion, the accomplishment of a digital forensic investigation case can be a complex and disorganized exercise, often leading to trust in invalid pieces of evidence or failure in the process or good framework leading to the reconstruction of such evidence. One of the most crucial aspects of digital forensics is evidence handling because it alone determines whether evidence will meet the requirements for legal admission in a court of law. Most of the time, digital evidence can be collected with ease thanks to a proper chain of custody. The tricky part is keeping it safe from tampering, cyberattacks, and data breaches. It is very challenging to prevent these attacks and detect tampering as it is done discreetly to make it seems like it is still intact. Based on that, some of the vital considerations were highlighted to provide areas for contemporary research aiming to improve and efficiently enhance digital forensics implementations and investigations process, especially for cybercrimes.

CHAPTER FIVE
SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This sections summaries the major the findings of the research in this regards forming a basis for appropriate recommendations plus conclusions with an aim of answering the research all questions. Challenges and limitations of this study are also highlighted in this section.

5.2 Summary of Findings

The study aimed to develop an efficient digital forensics framework for combating cybercrime. Additionally, the study aimed to assess existing frameworks used for combating cybercrime with a view to identify existing gaps, to develop an efficient framework for investigating digital crimes based on the universal standard for digital forensic investigation ISO/IEC 27043:2015 and finally to validate the developed framework and evaluate its performance compared to other existing frameworks. According to data analysis, 82.90% of respondents agreed that Communication Authority of Kenya should use an very effective digital forensics framework in its forensic investigations to combat cybercrime cases . Similarly, the Wycliffe Comprehensive Digital Forensic Investigation Framework was found to be superior to existing frameworks for digital forensics crime investigations.

5.3 Limitations of the Study

The major limitation of the study was that the Wycliffe Comprehensive Digital Forensic Investigation Framework is in still in the conceptual stages as well at a theoretical level and due to the limit of time more advanced research needs to be done to develop it into a program

5.5 Conclusions

It is difficult to use automated methods for collecting, identifying, extracting, analyzing, and presenting electronic evidence in the field of digital forensics and investigations. Even though it was possible to determine that digital forensic investigations require an very effective framework, it is important to note that this is only the most suitable location for the acquisition and transportation of digital evidence collected from the site for subsequent analysis.. Similarly, the WFDCID framework which was indicated to be an effective framework requires

a significant amount of time to be able to analyze the image and generate forensic a compressive digital forensics report.

While the digital world of today is increasingly becoming an important component of any criminal investigation, it is essential to keep in mind that merely utilizing tools and possessing technical skills is typically not sufficient to thoroughly and appropriately investigate a digital crime. Digital forensic examiners must adhere to a well-defined procedure that goes beyond technical requirements. As a result, we must examine previous efforts and forensic frameworks in depth. To provide a clear framework for analyzing and reasoning about the requirements of digital forensics and investigations, a formal and methodical approach is required. Anti-digital forensics investigations cases situations and procedures also make the forensic investigation process difficult by contaminating any stage of the process, its requirements, or destroying the evidence.

REFERENCE

A Brief History of Forensic Science—MozartCultures -now.htm. (n.d.).

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). *Systematic Digital Forensic Investigation Model*. 14.

Al-Dhaqm, A., Abd Razak, S., Othman, S. H., Nagdi, A., & Ali, A. (2016). A GENERIC DATABASE FORENSIC INVESTIGATION PROCESS MODEL. *Jurnal Teknologi*, *78*(6–11). https://doi.org/10.11113/jt.v78.9190

Almarzooqi, A., & Jones, A. (2016). *Applying grounded theory methods to digital forensics research*. 20.

Ankit Agarwal, Megha Gupta, Saurabh Gupta, & Prof. (Dr.) S.C. Gupta. (2011). *Systematic Digital Forensic Investigation Model*. *5*(5).

Aziz, B., Blackwell, C., & Islam, S. (2013). A Framework for Digital Forensics and Investigations: The Goal-Driven Approach. *International Journal of Digital Crime and Forensics*, *5*(2), 1–22. https://doi.org/10.4018/jdcf.2013040101

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cohen, L., Manion, L., & Morrison, K. (2009). *Research methods in education* (6. ed., reprint). Routledge.

CSS0080-guide.pdf. (n.d.).

Economic-espionage-1.pdf. (n.d.).

Etikan, I. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. https://doi.org/10.11648/j.ajtas.20160501.11

Flandrin, F., Buchanan, W. J., Macfarlane, R., Ramsay, B., & Smales, A. (2014). *Evaluating Digital Forensic Tools (DFTs)*. https://doi.org/10.13140/2.1.3293.6004

Gordon, G. R., Hosmer, C. D., Siedsma, C., & Rebovich, D. (n.d.). *Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime*. 114.

Hamed Taherdoost. (2017). Determining Sample Size; How to Calculate Survey Sample Size. *International Journal of Economics and Management Systems*, *2*, 237–239.

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*, 29–36. https://doi.org/10.1016/j.diin.2006.06.004

Kilungu, M. K. (n.d.). *An Investigation Of Digital Forensic Models Applicable In The Public Sector*. 96.

Kohn, M. D., Eloff, M. M., & Eloff, J. H. P. (2013). Integrated digital forensic process model. *Computers & Security*, *38*, 103–115. https://doi.org/10.1016/j.cose.2013.05.001

Krishnan, S. (2019). Role and Impact of Digital Forensics in Cyber Crime Investigations. *INROADS-An International Journal of Jaipur National University*, *8*(1and2), 64. https://doi.org/10.5958/2277-4912.2019.00012.2

Marshall, A. M. (2021). Digital forensic tool verification: An evaluation of options for establishing trustworthiness. *Forensic Science International: Digital Investigation*, *38*, 301181. https://doi.org/10.1016/j.fsidi.2021.301181

[No title found]. (n.d.). *International Journal of Information Security and Privacy*.

Pourvahab, M., & Ekbatanifard, G. (2019). Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology. *IEEE Access*, *7*, 153349–153364. https://doi.org/10.1109/ACCESS.2019.2946978

Raghavan, S. (2013). Digital forensic research: Current state of the art. *CSI Transactions on ICT*, *1*(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

Rahim, N., Wahab, A. W. A., Yamani, M., Idris, I., & Kiah, M. L. M. (n.d.-a). Digital Forensics: An Overview of the Current Trends. *Digital Forensics*, 14.

Rahim, N., Wahab, A. W. A., Yamani, M., Idris, I., & Kiah, M. L. M. (n.d.-b). Digital Forensics: An Overview of the Current Trends. *Digital Forensics*, 14.

Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers & Security*, *23*(1), 12–16. https://doi.org/10.1016/j.cose.2004.01.003

Role of Digital forensics in comberting cybercrimes.pdf. (n.d.).

Romagna, M. (n.d.). *HACKTIVISM AND WEBSITE DEFACEMENT: MOTIVATIONS, CAPABILITIES AND POTENTIAL THREATS*. 11.

Rothke, B. (2001). Corporate Espionage and What Can Be Done to Prevent It. *Information Systems Security*, *10*(5), 1–7. https://doi.org/10.1201/1086/43315.10.5.20011101/31716.3

Samuel, A. W. (n.d.). *Hacktivism and the Future of Political Participation*. 284.

Singh, D. A. (2014). *Cyber Forensics in Combating Cyber Crimes*. 3.

Sundresan Perumal. (2010). *Digital Forensic Model Based On Malaysian Investigation Process*. *9*(8), 8.

Taherdoost, H. (2016). Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3205040

University Of East London, & Ay, O. (2020). Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*(1), 1–8. https://doi.org/10.24966/FLIS-733X/100045

Uon, J. M. N. (n.d.). *Analysing The Efficiency Of Forensic Science Units Within Kenya*. 85.

APPENDICES

APPENDIX 1: RESEARCH BUDGET

It is important for a researcher to work out a budget and identify the required costs that will help accomplish the project.

No.	Description	Amount
1	Proposal Typesetting and Printing 50pgs @50	2,500/=
2	Stationery	3,000/=
3	Questionnaire Preparation and Testing	3,500/=
4	Data Collection Traveling Expenses	12,000/=
5	Data Analysis (Software Hire)	5,000/=
6	Typing and Report Binding	10,000/=
7	Airtime and Communication Expenses	3,000/=
8	Subsistence	5,000/=
9	Contingencies	4,400/=
	Total	**48,400**

Source: Researcher

APPENDIX 2: RESEARCH SCHEDULE

A schedule shows each activity of the research and helped the researcher see at a glance which tasks should be done at what time to enable them complete on time. The schedule helped the researcher to come up with a list of milestones that when achieved will help them move to the next steps leading to the final completion.

	May - June 21	**Aug 21**	**Sept 21**	**Oct-Apr 22**	**May 22**	**Jun 22**	**Jul 22**	**`Aug 22**	**Sep 22**
1. Topic Identification									
2. Approval of Topic									
3. Concept Development									
4. Chapter One – Introduction									
5. Proposal Literature Review and Methodology									
3. Proposal Presentation									
4. Defense									
5. Submission of a Proposal									
6. Questionnaire Pre-Testing									

7. Data Collection , analysis & Processing									
8. Submission of done Project Report									

APPENDIX 3: QUESTIONNAIRE

Kindly provide correct and useful data and fill appropriately as logically guided. (This Questionnaire has been provided as a word document that can be filled out in soft copy and returned via e-mail; or google forms.

SECTION 1: GENERAL INFORMATION

1. Gender of the respondent (Tick ( ) Male ( ) Female ( )
2. Highest level of educational qualification (tick)

a) Secondary education [ ] b) Certificate or diploma [ ]

c) Graduate [ ] d) Postgraduate [ ]

3. How many years have you been involved in forensic investigation in Kenya?(tick)

a) Less than 1 Year [ ] b) 1-2 Years [ ]

c) 2-3 Years [ ] d) 3-4 Years [ ]

d) 4 Years and above [ ]

4. Would digital forensics framework enhance efficiency of digital forensics investigation work?
   Yes [ ] No [ ]
   If Yes explain

   ……
   ……

5. Are the forensic investigation equipment adequate and reliable in collecting evidence from the crime scene? Yes [ ] No [ ]
6. Do you think it is adopting a clear chain of custody when performing digital forensic investigations improves the investigation process? Yes [ ] No [ ]

   If Yes explain

   ……
   ……

7. Do you think it is important to encrypt evidence through hashing?
   Yes [ ] No [ ]

   If Yes explain

   ……
   ……

8. Do you think reconstruction of the crime-scene is an important test to test investigative hypothesis and improve the integrity of the crime scene?
   Yes [ ] No [ ]

   If Yes explain

   ……
   ……

9. Do you think absence of standard digital forensics investigations frame influence investigations process?
   Yes [ ] No [ ]

   If Yes explain

   ……
   ……

10. Do you think importance documentation, results and reporting in digital forensics investigations is important practice in digital forensics framework.
    Yes [ ] No [ ]

    If Yes explain

    ……
    ……

11. Do you think following a forensic investigation framework's guidelines speeds up the investigation process and gives more accurate findings?
    Yes [ ] No [ ]

    If Yes explain

    ……
    ……

Framework	**Frequency**
The Systematic Digital Forensic Investigation Model	
Digital Forensic Model Based on Malaysian Investigation process	
Wycliffe Comprehensive Digital Forensic Investigation Framework	
Integrated Digital Forensics Process Model	

12. Which of the following Digital Forensics and Investigations Frameworks is reliable in production of Concrete Evidence

13. In a scale of 1-5, how efficient, reliable. Accurate and comprehensive the following frameworks when conducting digital forensics investigations. 1 Being the lowest (poorest) and five being the best.

Framework	**scale**
The Systematic Digital Forensic Investigation Model	
Digital Forensic Model Based on Malaysian Investigation process	
Wycliffe Comprehensive Digital Forensic Investigation Framework	
Integrated Digital Forensics Process Model	
Total	