AN EXPLORATION OF VIRTUAL CRIMINAL INVESTIGATIONS IN GHANA: LEGAL ISSUES AND CHALLENGES

by

AUGUSTINE AMOAKO
Student No: 46473742

submitted in accordance with the requirements for

the degree

of

DOCTOR OF PHILOSOPHY

in the subject

CRIMINAL JUSTICE

at the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: DR. B. K. LEKUBU
CO-PROMOTER: DR T.L. MABUSELA

JUNE 2023

Open Rubric

ACKNOWLEDGEMENT

I would like to thank my supervisors DR. B. K. LEKUBU and DR. T. L. MABUSELA for their guidance and advice throughout this thesis. Through the guidance of DR. B. K. Lekubu and DR T. L. Mabusela I was able to focus on my arguments and structure my research. They also greatly assisted in identifying gaps in this study and areas for improvement. I am also thankful to the former Chair of Department of Criminal and Procedural Law (Dr. T. Mokoena). Another appreciation goes to former Chair of Police Practice Department (Dr. L. Motsepe) for their effort in locating these extra-ordinary supervisors for me. A special word of thanks also goes to my parents, brothers, wife and children for their encouragement and prayers.

DECLARATION OF ORIGINALITY

I, Augustine Amoako (student No: 46473742), hereby declare that this thesis titled "**AN EXPLORATION OF VIRTUAL CRIMINAL INVESTIGATIONS IN GHANA: LEGAL ISSUES AND CHALLENGES"** has not previously been submitted by me for a degree at any other university; that this is my own work in design and execution and that all material from published sources contained herein have been duly acknowledged.

AUGUSTINE AMOAKO

NOVEMBER 2022

PRETORIA

ABSTRACT

The widespread cybercrime has caused changes and brought about a need for new investigative skills, laws and enforcement procedures to attack these obstacles. Since technological crimes committed through the information superhighway or the internet is evolving very rapidly, efficacious enforcement of cybercrime is becoming extremely challenging. Cybercrime is both a national and international issue and local legislation alone cannot be able to combat the menace. Digital evidence permeates every aspect of the average person's life in today's society and no matter what you are doing these days, a digital footprint is probably being created and contains some type of digital evidence that can be recovered through digital forensic investigation It requires stringent laws, skilled personnel, well-established institutions, and transnational response. To efficaciously combat cybercrime, countries, states or governments must establish an independent anti-cybercrime unit and design national guidelines for digital evidence collections to combat the canker. This thesis, therefore, presents an examination of the virtual crime or cybercrime investigation challenges and legal issues on electronic evidence in Ghana. The study examines the existing cybercrime laws and practices in Ghana and makes a comparative study from other jurisdictions. Also, the study draws a survey from the international legal framework on cybercrime and electronic evidence on various methods and procedures that can be used to conduct digital forensic search and seizure of electronic evidence and investigation when cybercrimes occur. Recommendations were made which include formulation of stringent laws, establishing the national Cybercrime investigation Strategy and policies, the establishment of national guidelines for digital evidence collections, develop anti-cybercrime tool-kit for the collection of digital evidence, the establishment of digital forensic training institutions in all regions of Ghana for hands-on skilled based training for law enforcement officers and judges to ensure efficiency in the process of digital forensic investigation and prosecution of cybercrimes in Ghana are given.

Keywords: Cybercrime, Digital Forensic, Investigation, Tool-kit, Electronic Evidence.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ACPO	The Association of Chief Police Officers
ACSC	Australian Cyber Security Centre
APEC	Asia-Pacific Economic Cooperation
ATM	Automated Transaction Machine
AU	African Union
CART	Computer Analysis and Response Team
CDA	Communication Decency Act
CERT	Computer Emergency Response Team
CERT	Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
CFAA	Fraud and Abuse Act
(CIPRO)	Companies and Intellectual Property Registration Office
CFRF	Cloud Forensic Readiness Framework
CSAM	Child sexual abuse material
CID	Criminal Investigation Department
CIPRO	Companies and Intellectual Property Registration Office
CNCI	Comprehensive National Cybersecurity Initiative
COE	Council of Europe
CPPA	Child Pornography Prevention Act

CPPA	Congress’s Child Pornography Prevention Act
CPS	Crown Prosecution Service
DFRWS	Digital Forensics Research Workshop
DOJ	Department of Justice
DoS	Disk Operating System
DoS	Denial of Service
DPA	Data Protection Act
DPA	Data Protection Act
DPC	Data Protection Commission
DPP	Director of Public Prosecutions
DVD	Digital Versatile Disks
ECA	Electronic Communication Act
ECPA	Electronic Communication Privacy Act
ECTF	Electronic Crimes Task Forces
EOCO	Economic and Organized Crime Office
EPCIP	European Program for Critical Infrastructure Protection
ETA	Electronic Transaction Act
FBI	Federal Bureau of Investigation
FSL	Forensic Science Laboratory
FT	Forensic Tools
FTC	Federal Trade Commission
FTK	Forensic Tool Kit
GPS	Global positioning systems
HSPD	Homeland Security Presidential Directive

ICE	Immigration and Customs Enforcement
ICT	Information and Communication Technology
ICT4AD	Information Communications and Technology for Accelerated Development
IDIP	Integrated Digital Investigation Process
IDS	Intruder Detection System
IGP	Inspector General of Police
IoT	Internet of Things
ISO	International Organization for Standardization
ISP	Internet Service Providers
ITAA	Information Technology Agency Act
LA	Legal Authorisation
MD	Message Digest
NCSC	National Cyber Security Centre
NIIP	National Information Infrastructure Protection
NIJ	National Institute of Justice
NIST	National Institute of Standards and Technology
NITA	National Information Technology Agency
NITAA	National Information Technology Agency Act
NSPD	National Security Presidential Directive
PA	PROTECT Act
PDD	Presidential Decision Directive
PIPCU	Police Intellectual Property Crime Unit
PNDCL	People National Defense Council Legislation

PPA	Privacy Protection Act SOPs Standard Operating Procedures
RCLs	Computer Forensic Labs
SA	South Africa
SSA	Social Security Administration
USA	United States of America
UNODC	United Nations Office on Drugs and Crime
UKACPO	United Kingdom Association of Chief Police Officers
UK	United Kingdom
UN	United Nation
USPIS	United States Postal Inspection Service

CHAPTER ONE

BACKGROUND TO THE STUDY

1.1 INTRODUCTION

Computer technology and the digital information age have become a ubiquitous part of modern life and it brought with it opportunities, possibilities and challenges that were barely imagined generations ago. For this study, it is to be observed that the global nature of the internet has presented difficulties in investigations for prosecution concerning cyber criminality. “(Basdeo Montesh & Lukubu, 2014)” state that investigating and deterring cyber-crimes, and imposing legal sanctions on cyber-criminals warrants an international legal framework. There has been an exponential growth of information communication technology infrastructures including computer networks and information superhighways which has also created increasing opportunities for potential offenders as well as multiple risks for potential victims. These criminal activities conducted on the information superhighway are characterised among other things as computer crime, virtual crime, cybercrime, internet crime, information technology crime, high-tech crime, electronic crime, and dark web crime.

Information technology crime does not require physical proximity between the victim and the perpetrator for the commission of the crime (Basdeo et al, 2014:48)**.** The administration of justice occupation is not keeping pace with the high-tech crime and another electronic infrastructure context. Basdeo et al (2014:48) affirm in their research that the effects and impact of information technology on the legal system have not yet received the attention they warrant and challenges presented by the electronic realm cannot be solved merely by imposing existing criminal and criminal procedural laws which govern the physical world on cyberspace. Online activities with millions of computers and connectivity to the internet are vulnerable to the threat of cyber-criminal activities. For instance, individuals conducting online transactions face online credit card fraud which is an escalating issue owing to numerous skimming, ransomware, counterfeiting and

phishing schemes which transpire throughout each year costing co-operations, institutions and victims billions of dollars. Moreso, whilst the Internet offers a multitudinous upper hand and opens up new channels for transaction business, it also has brought in an enlarged likelihood of cyber fraud in electronic cash and credit card transactions. Recently, the face of high crime has altered as a result of the advent of the new electronic environment, organized gang cybercriminal groups**.** The amalgamation of creative online criminals and widespread of sophisticated electronic devices and existence of broadband internet-based information systems and connectivity throughout the world has compounded vulnerabilities of online crimes. Given this, the evolution of reachable information and communication technologies and the extension of the internet-based information systems technologies have led to multitudinous new criminal behaviours. Whilst mankind enjoys the rapid growth of information and communication technology, it has also given the rise to virtual or cyber-crimes. Criminals are now operating from any part of the world without restrictions of territorial boundaries on the Internet.

According to Raghavan and Parthiban (2014:173) there are several e-fraud types witnessed in the banking sector like Automated Teller Machines (ATM) fraud, cyber money laundering and credit card fraud and in general, all the fraud types are executed with the ultimate goal of gaining access to the users' bank account. Hackers and crackers attack servers to commit virtual crimes such as stealing passwords, credit card information and other confidential or secret information; to intercept transactions and communications, and to cause damage such as mutilation of websites or to corrupt or insert viruses into the database of the target server. It is the submission in this study that virtual criminal activities have made digital forensic investigations increasingly important.

Notably, virtual crime was uncommon twenty-five (25) years ago in Ghana, but swift advances in digital infrastructures, the promotion of personal computers, and easy internet accessibility have changed the way crimes are committed and the way law enforcement conduct investigation. There have been many endeavours or attempts to tackle and address high-tech crime in the law but they are thwarted by the speed at which technology changes compared to the rate at which laws are created or revised. For example, the communication minister Mrs Usula Owusu reported that Ghana had 7.9

million internet users in 2017 and 2019, it recorded a total of 10.3 million users, representing a three (3) million increase in the spate of two years. It is interesting to note that as of January 2022, Ghana had approximately 17 million internet users registered, and the number of Ghanaians using the internet is growing exponentially. The Ministry concluded in its final draft report on Cyber Security Policy that "even though the Electronic Transaction Act (ETA) has provisions for law enforcers to address cybercrime, however, this is not adequate and it does not address fully all aspects of cyber security challenges, especially the multi-stakeholders approach" (Ministry of Communication 2014). Electronic Transactions Act, 2008 (Act 772), hereinafter ETA, accordingly needs to be reviewed to fully address all challenges emerging in the cyber ecosystem. The face of cybercrime has changed recently as a result of new Internet environments, organised cybercrime groups, and new "smart" viruses (Cassim, 2009:123). The increasing incidents of cyber-attacks against the state and critical information and communication infrastructures necessitate a national response. It is incontestable that the fundamental purpose or cause of the criminal investigation functions in the 21st century has for the most part remained unchanged. Virtual crime requires few resources to be committed in any jurisdiction without the offenders being present at the physical location; hence it differs from traditional crimes investigation and is a prime endorsement of the Ghana Police Service.

Matters that concern the police are exclusively legislative competence in that the police institution is to be organised and administered in accordance with the Police Force Act (Act 350) which was enacted in 1970. The Police Force Act (Act 350) stipulated in Section (1) that "it shall be the duties of the Ghana Police Force to prevent, detect and investigate crime, apprehend offenders and to maintain public order and safety of persons and properties. One of the inherent duties or roles of police in common law jurisdictions such as Ghana is investigations, and this is in line with the Anglo-Saxon adversarial justice system wherein the executive arm of government as represented by the police, conducts investigations in relevant situations to establish a *prima facie* case prior to prosecution. Understandably, the Criminal Offence Act, 1990 (Act 29), and the Criminal Offences Procedure Act, 1960 (Act, 30) have been enacted to enhance law enforcement investigations into criminal behaviour and crimes. However, both acts inadequately cover cyber-related crimes. No sections or provisions are claiming to warrant or authorize

cybercriminal behaviour and the gathering of appropriate digital evidence for virtual crime prosecution. The investigation and evidence gathering on the crime committed through electronic communication for criminal prosecution is not an easy task. In 2008, the government of Ghana instituted the Electronic Communication Act, 2008 (Act 775), hereinafter ECA, to deter virtual attacks on communication infrastructures but this legislative framework is not sufficient, and it is inefficient to address other virtual crimes. Procedural rules used by law enforcement agencies such as the police do not ensure that the collection and further processing of electronic evidence comply with the provisions guaranteeing data protection and communication secrecy. With the widespread concern about internet privacy, the government of Ghana also enacted the Data Protection Act in 2012 (Act 843), to enhance the protection of individual data in the virtual environment. Again, this law is silent and does not have all the specific provisions to regulate privacy concerns of individuals despite widespread agreement on the need for privacy protection in the virtual world. As claimed by the newspaper called Daily Graphic (2019), “data in the wrong hands have caused untimely death and jeopardised many lives.” Therefore, strong provisions must be made to protect people against abuse by those institutions that keep their information on the internet such as schools, hospitals and governmental organisations (Daniel, Ronald & Mensah 2019:36)

Larry and Lars (2012:40) state that the primary purpose of digital forensics is to present digital evidence in legal proceedings. Digital forensic evidence is used in many ways in legal matters not only as part of civil and criminal trials but also during the pre-trial and post-trial phases. Therefore, techniques such as drive imaging, employed to extract digital evidence from devices must comply with legal standards. Virtual criminal investigations are not constrained by geographical boundaries and legal issues are complicated by the presence of multiple jurisdictions even though there have been investigations done by Interpol and Europol through mutual legal assistance or memorandum of understanding among countries. Jurisdiction in cybercrime is a tricky issue (Eoghan, 2013:18). The internet transactions that are legal in the state where they are initiated may be illegal in other states, even though the act is not particularly targeted at that particular state. Cybercrime statutes that have been enacted over the past decades in numerous countries show varying and diverging jurisdiction clauses (Brenner and Koops 2004:201).

Some countries even go so far as to claim jurisdiction based on very indirect links with their territory (Eoghan, 2013:192). Malaysia, for instance, has established jurisdiction in Article 9 of its Computer Crime Act 1997 as follows: this Act shall apply if, for the offence in question, the computer, programme or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time. Communications laundering, which involves routing transmissions through a series of jurisdictions to frustrate attempts to trace the source, or the extensive use of cryptographic techniques to render data unintelligible are usual steps, taken by cyber-criminals, to hide or disguise their activities (Walden, 2005:58). Despite the available legislations or laws in fighting against virtual crime, the virtual criminal forensic investigations for gathering electronic evidence to support prosecution have not been fulfilling the expectations and are not satisfactory as well and therefore the cooperation between states or countries is key to ensure that investigation and prosecution of virtual crime are not defeated by jurisdictional issues.

Less than two decades ago most individuals did not own a cellphone or personal computers. Internet connectivity was possible through dial-up modems or Ethernet cabling, and people paid by the hour for access to the web. Video game systems were using 16-bit graphics and they did not connect to other devices. Global positioning systems (GPS) were largely used in military applications only. It is amazing to consider that the world and human behaviour have changed so quickly through the use of technology. In 2016 there were 3.4 billion Internet users worldwide comprising 46.1 percent of the world's population “(Internetlivestats, 2016)”. China has over 500 million smartphone users, while India has only 125 million users, and as these rates continue to increase, Internet use will change, hence, transforming social and economic interactions in unique ways from country to country. For instance, 77 percent of Americans owned a smartphone and used video sharing sites as of 2016, with substantial access among younger populations particularly African American and Hispanic users, which attribute to the increase. With the advent of new technology, new types of crime have surfaced and traditional crimes such as fraud are now perpetrated through sophisticated technology (Maat, 2009:145)

Cassim (2009: 76) affirms that an important challenge to state officials in prosecuting cybercrime is one of jurisdiction. Traditional boundaries have fallen away and a virtually borderless world has become a platform for crime (Cassim, 2009:76). Criminal laws regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cyber criminals in different countries across different jurisdictional borders (Brenner, 2011). Today's cybercrime activities focus on utilizing globalized information communication technology for committing criminal acts with transnational reach "(United Nation Office on Drugs and Crime Comprehensive study on cybercrime, 2013)". According to Satola and July (2011:230), cybercrime is perhaps one of the more clearly identified thematic areas of cyber security and the one where there is almost universal agreement on best practices, as expressed in the Council of Europe Convention on Cybercrime "(Budapest Convention, 2001)."

The word "Cybercrime" is on the lips of almost everyone involved in the use of the computer and Internet, be it individual, corporate, organization, national, multinational or international. Cybercrime raises issues of privacy, or rather, the increasing loss of privacy (Susan, 2010:221). Thomas and Adam (2016: 211) emphasized that the use of the computer for legitimate activities from banking and social networking to searching for employment is a commonplace, almost taken for granted aspect of modern life. However, the information that we send into cyberspace makes us vulnerable to cybercrime. There have been crimes committed such as hacking; internet fraud, identity theft, phishing and pharming which have become major issues. The internet, computers, and mobile technologies have dramatically reshaped modern society. Virtual crime or cybercrime or "e-crime" or "computer-related crime" or "digital technology crime" is a long-established phenomenon. Cybercrime (online misdemeanour) has been defined as including any crime carried out primarily using a computer on the Internet; for example, hacking into or damaging a computer network, accessing and stealing electronic data without authorization, and cyberstalking (via e-mail threats of violence or extortion). Criminal activities that involve the use of computer either as an instrument, target or a means to carry on further crimes comes within the confines of cybercrime.

The cybercrime menace in Ghana had been more of cyber fraud popularly called “Sakawa," where cyber criminals tend to dupe unsuspecting internet users from Ghana and abroad for large sums of money. These crimes remain prevalent because of inadequate laws on cybercrime investigations and the gathering of electronic evidence for prosecuting cyber criminals. Del Aden (2018) made a remark at the 4th edition of the Ghana Cyber Security Workshop in the citi business news, that the incidence of cybercrime in Ghana will continue to rise unless businesses put effective counter measures in place, and added that with increased digitization, the risks related to cyber security naturally increase (Citifmonline, 2018).

1.2 RATIONALE OF THE STUDY

This research is designed to identify the prevalence of virtual crimes in Ghana, and forensic investigation weaknesses and challenges for law enforcement officers, prosecutors, and other business organizations to improve upon their investigating methods and to come up with strict investigations framework or methodologies and legislations for the prosecution of cybercrime in Ghana.

As commented by Cassim (2009:36) the traditional law enforcement tools such as handcuff, baton, firearms, and ammunition are regarded as ineffective in addressing these crimes. Law enforcement officers not having enough of a specified quality virtual criminal forensic tool for gathering evidence when the digital crime scene is identified, poses a challenge and this is because it is a new area in Ghanaian criminal jurisprudence, hence lack of rules and guidelines established on prosecutions that regard as an example to resort to in prosecuting cases of such nature. Even though there are judicial officials who have experience in the evidentiary material presented in court, there are still many of these judicial personnel and judges who lack the technical terminologies and understanding of cyber legal technology and have not also received enough training on how to handle cases on virtual crimes for prosecution especially and this poses a challenge. The cross-border Internet and its online spaces span a fragmented patchwork of national jurisdictions. As connectivity and Internet penetration increase, so do the conflicts between jurisdictions (Citifmonline, 2019). The fact that cybercrime does not

require physical proximity between a victim and perpetrator also compounds the problem of detection (Cassim, 2009:40). Enforcement of a country's criminal laws can be thwarted by other countries deliberately. Without the corporation of the government of a nation, processing electronic investigations and evidence gathering can be difficult. The refusal by countries like Russia and China to extradite their citizens, for example, has repeatedly proven an obstacle to prosecution (Mirovalev and Colin 2005). Domestic criminal law is thus often an ineffectual tool when it comes to bringing foreign cyber criminals to justice.

The challenges deriving from cybercrime arise in four main areas: logistics, combating anonymity, accessing electronic information and transnational enforcement (Allan, 2005:150). Due to scanty budget allocation to law enforcement on technological developments there is an inadequate number of Cyber Police force officers or Cyber law enforcement and security experts trained in detecting, investigating, and eradicating virtual crime, and this means that organizations and agencies remain at risk from virtual-attacks. As nations across the globe strive to curb cybercrimes through the instrumentality of the law on digital forensic investigation, so are the cyber criminals devising new and sophisticated techniques to further their trade, thereby rendering impotent legal measures (Ajayi, 2015).

A report released by the Kenyan-based IT firm, Serianu Limited in 2017, revealed that Ghana's economy lost a total of US$50 million to cyber-crime in 2016, and the breakdown of the report shows that Nigeria recorded the highest figure of US$550 million, followed by Kenya and Tanzania with US$175 million and US$85 million respectively. Ghana and Uganda also recorded US$50 million and US$35 million respectively "(africabusinesscommunities.com/news/ghana-loses-$50m-to-cyber-crime-report/,2017)." The Minister of Communication disclosed that the criminal investigation Department (CID) estimates that in the reported cases of cyber incidents, victims both individuals and businesses, Ghana lost about $105 Million in 2018. The cybercrime unit of Ghana Police Service (2020) states that in 2019 Ghana lost $9.8 Million to cyber criminals as against $105 Million in 2018 and out of the amount, $6.8 Million was lost through fraud, $2.7 lost to intrusion and stealing, and rest to sextortion and child pornography (ghanaweb, 2020). Yankson (2020) stated that cybercrime topped the 192

reported cases to the unit representing forty-seven percent (47%). This figure excludes indirect costs as well as other incidents which were not detected and or reported to law enforcement and other regulatory bodies. Reported cases of cybercrime include hacking into protected databases systems, business fraud, social media, impersonation or identity fraud, ransomware attacks, data leakage or breaches and online safety breaches involving children (Ghanaweb, 2020). The lack of successful investigations and prosecutions of cybercrime-related cases and the lack of relevant and up-to-date legislation to address issues of digital forensics and electronic evidence, knowledge and relevant judicial authorities also pose a challenge as well as the lack of domestic expertise are all key indications affecting Ghana in virtual environment activities.

1.3 PROBLEM STATEMENT

Creswell (2014:108) indicated that a problem statement is the heart, clear statement supporting evidence of the research project that leads to the need for an in-depth research study and analysis in the environment to be addressed. problem statement is defines as an area of concern of the research to be improved upon identifying what is probably necessary to conduct the study and explaining how the finding will present conceptual ideas to concrete action to resolve the problem. Bless, Higson-Smith and Sithole (2014:41-43) claimed that selecting a research problem is a delicate task because out of the great variety of queries arising from the environment, one must sort out the ones appropriate for scientific investigation. Also, Babbie and Mouton (2012:73) posited that all research starts with the identification and clear formulation of a research problem and it is often formulated in the form of either a research question or a research hypothesis. Again, Babbie and Mouton (2012:78) made it clear that a good and clear research problem outlines the purpose or aims of the study as well as what the objects of the investigation will be. Acquiring more information on an issue or problem helps to explain the relationship between the existing facts hence identifying a problem.

Despite the successfulness of click-and-mortar, pure-play or virtual businesses and e-government in the country's economy, Ghana is still gaining a bad reputation for virtual

crimes or cybercrimes. The country is ranked 6th representing 5% of malware attacks and 8th representing 4% of spam attacks in African virtual crime or internet crime (Symantec, 2019) This determines show Ghanaians are engaged in virtual or cyber fraud, ranging from hacking of official sites, mobile money fraud, spam and denial of service attacks, online gold fraud and other virtual or digital technology crime. According to the Ministry of Communication, about 82 virtual or cyber-crimes occur in Ghana every month and which is an average of 1000 crimes a year (GhanaWeb, 2019). Deloitte and Touché, IT Auditor, Jesse Arthur cited the lack of password policy by companies and deterring legislation among the challenges facing the country in addressing cyber security issues (GhanaWeb, 2019). What is more distressing about the growing incidence of virtual crime was the fact that a lot of young people are among the perpetrators of these criminal activities (Dailygraphic, 2013). The existing cybercrime laws enacted in Ghana are insufficient to deal with cross-border cybercrimes amid surging global threats.

The Government of Ghana, in its quest to bring virtual crime to the barest minimum, instituted or enacted a sleuth of legislation that directly and indirectly deal with cyber-crime. This was in recognition of the threat cybercrime is posing to Ghana. As already indicated above, this legislation included ETA, ACA, and the Data Protection Act 843 of 2012. There has also been the National Information Technology Agency Act 771 of 2008. Some of the regulatory provisions are found in the Criminal Code. The primary objective of the ETA, for instance, is to secure cyberspace as a means of mitigating crime incidence that may affect the ability of citizens to create worth. The categories of clauses in ETA include electronic transactions, consumer protection, protected computers and critical database, the liability of service providers and intermediaries, cyber inspectors, cyber offences, and miscellaneous matters. The problem is that these acts notwithstanding the spirit with which they were enacted have proven to have limitations. Although ETA, for instance, enhances digital transactions or communications in the public interest the challenges in accessing electronic evidence from corporate bodies and service providers are not adequately addressed (Obobisa, 2013). Further, although, section 103 of ETA mandates service providers to keep logs and records of the name, electronic source and destination address, billing records if any, duration of service to a subscriber or customer, types of services and related logs of the subscribers, activities which takes place on its

electronic platform as may be reasonably appropriate for a period of twelve months and despite this provision in the law, this requirement is not enforced because many law enforcement officers are not aware of this provision and the powers they have to demand compliance from service providers (Obuobisa, 2019).

Currently, Ghana is facing several cases of virtual criminal activities such as revenge porn, e-fraud, mobile-payment fraud, phishing, and offences relating to national interest and security. There are also cases of the internet being used to harm competitive businesses according to the police (Obuobisa, 2019). The limitations of the acts intended to deal with cyber activities are the Achilles heels in dealing with cybercrimes, so is generally the lack of full competency of judicial systems to understanding the environment of the cybercrime. For instance, even though there are judicial officials who are experienced in the evidentiary material presented in court, there are still many of these judicial personnel and judges who lack the technical terminologies, cyber legal technology and training on how to handle cases on virtual crimes for prosecution and this poses a challenge but the difficulty is how to trace the primary source of evidence. Law enforcement institutions are incapable or lack the necessary skills for virtual criminal investigations when cybercrimes occur. These limitations of the criminal justice system in Ghana have been appreciated and acknowledged by the Acting Director of Public Prosecution in Ghana who stated concerning cybercrime that there is improper handling of electronic evidence and goes further to explain that some investigators lack experience in the gathering of electronic evidence in compliance with court admissibility rules (Obuobisa, 2019). This has often resulted in very important evidence being dismissed as inadequate by the courts, hence the consequences of Ghana's image being dented as a virtual-crime-pronged location. Thus the country continues to see the proliferation of both technical and non-technical cybercrime perpetrators (Ennin and Mensah, 2019). The situation remains largely unabated and is largely aggravated by several factors including inadequate computer crime investigators, lack of ultramodern equipment in the investigation of cyber-crimes, and lack of cooperation from the Internet Service Providers and authorities in other jurisdictions in investigations by Ghana Police Service and the prosecution authorities.

1.4 AIMS AND PURPOSE OF THE RESEARCH

Primarily, the aim and purpose of this research is to identify the widespread of virtual crimes in Ghana, and digital forensic investigation challenges and frailty for law enforcement officers, security officers, prosecutors and other business organisation to improve upon their investigative procedural and electronic evidence gathering methods and to come up with legislations framework for cybercrime prosecution in Ghana. The statement of purpose of the research provides the major objective or intent or "road map" of a study (Creswell, 2013:134). Likewise, Locke, Spirduso and Silverman (2014:214) posit that research aims need to be clear, specific and concise. In simple terms, the aim and purpose of the research are discovered by asking the question: "What is my research for?" (Mason, 2002:20). Berg and Lune (2012:8) state that the purpose of study or research is to discover answers to questions through the application of systematic procedures. According to Thomas (2013:6-7), the circumstances of the researcher may affect the purpose of the research and the researcher may conduct research to: Find something out for its own sake; evaluate something; find out if something works, and improve the researcher's own or others' practice. Mouton (2014:101) states that the research purpose gives a broad indication of what the researcher wishes to achieve in their research. The three common and useful purposes of social research are: Exploration, description and explanation (Babbie and Mouton, 2012:79). Fouch and Delport (in De Vos et al., 2011:107) state that the aims and purpose of the study must be valuable for the intended target group, it must be able to discover new useful information that will add improvements to knowledge, practises and policies in the particular field of research. The widespread use of electronic payments systems such as mobile money has increased tremendously and to eliminate or combat virtual crime which hinders cyber commerce activities, the research will try to identify weaknesses and challenges for law enforcement officers, prosecutors, and other business organizations to improve upon their investigating methods and to come up with strict legislations for the prosecution of cybercrime. To this end, the study on “An Exploration of Virtual Criminal Investigations in Ghana: Legal issues and challenges” is of importance towards contributing to the discourse on combating and prosecution of virtual or cyber criminals in light of the

exponential growth of digital businesses or electronic commerce industries in Ghana. The people in Ghana prefer to transact business activities online.

1.5 RESEARCH OBJECTIVES

Mouton (2014:101) indicates that the existing background knowledge and the interests, motives and preferences of the researcher are the sets of factors that co-determine the clarification of the research objective. Mouton (2014:101) further states that the research objectives give a broad indication of what researchers wish to achieve in their research. According to Kumar (2014:69) objectives are the goals the researcher set out to attain in the study. The objective of this study is to examine and identify legal issues and challenges relating to virtual criminal investigations and to do a comparative legal study of other jurisdictions under study which includes South Africa, United Kingdom, United States, and Australia. Each objective should describe only one issue.

The following are the specific issues addressed in this study:

1. To identify legal issues and challenges of virtual criminal investigation in the existing laws governing cybercrime.
2. To inquire into the existing cybercrime legislation principles and their application towards digital forensic investigation and admissibility of virtual evidence for prosecution.
3. To identify the main problems in ensuring the integrity of digital evidence in digital forensic investigations.
4. Conduct comparative studies of anti-cybercrime legal and investigation methodologies and strategies in countries that are known to have effective anti-cybercrime strategies in place.
5. Make suggestions and recommendations intended to help the country develop and design effective and efficient anti-cybercrime investigations and prosecutions framework.

1.6 RESEARCH QUESTIONS

Bryman and Bell (2015:10) indicate that a research question addresses an unequivocal announcement of what the researcher needs to know. Gilbert (2008:44) emphasises that the research question is integral to the design of a research project overall and a critical stride during the time spent completing a research project. Denscombe (2015:92) explains that the research questions must be precise and point out what needs to be investigated, adding further that the research questions provide the basis for what data to be collected, as they pose questions that are vital for addressing the key concern of the study. Bryman (2012:9) claimed that the research question provides an explicit statement of what the researcher wants to know about. Flick (2011:84) states that for the success of the study, it is important to limit the chosen research problem to the research question that is manageable as the decision on a research question will have implications for what will become the issue of the study, which aspects will be omitted, and which methods can be applied in the study. The three main types of research questions are exploratory questions: focus on a given situation or change; Descriptive questions: aims at a description of certain situations, state or process and Explanatory questions: focus on relations, more than just a state of affairs investigated (Flick 2011:26). Denscombe (2015:82) believes that research questions specify what factors and relationships will be investigated to provide data that will be useful in relation to research aims and objectives."

This study formulates the following research questions based on the specific objectives detailed in 1.5 above:

1. What are the legal issues and challenges of virtual criminal investigation in the current laws governing cybercrime?

2. What are the cybercrime legislation principles, and their application towards digital forensic investigation and admissibility of virtual evidence for prosecution?

3. Which problems are encountered in a digital forensic investigation relating to cybercrimes and how are these impacting the integrity of digital evidence?

4. What are the key national legislative framework and Ghana's regional and international obligations to combat Virtual crime or Cybercrime and to what extent, and based on which anti-cybercrime strategies, have other countries effectively been able to combat cybercrimes?

5. What are the successes and failures of the Ghana anti-cybercrime agencies in their fight against Virtual Crime and how can the legislative and regulatory framework in Ghana be improved to make them more effective and efficient in cybercrimes?

1.7 PHILOSOPHICAL WORLDVIEW OFFERED IN THIS STUDY

Creswell (2014:6) describes worldview as the basic set of beliefs that guide action. Olthuis (1985) cited in Fisher (2012:50) believes that the worldview is the paradigm in which reality is followed and managed; worldview provides an interpretation of an effective system by which order and disorder are judged. The types of beliefs held by the researcher often lead to embracing qualitative, quantitative or mixed methods approach (Creswell, 2014:6). Anderson (2014:52) submits that any research philosophy must address two fundamental and interrelated questions: How can we know the world and how do theories, concepts and experiences lead to knowledge? Swerdlin (2012:2) affirms that a worldview is a set of beliefs and added further that these beliefs are used to make sense; filter reality is the accumulation of experience of assumptions of what may be realities and beliefs that are true, partially true or false (Fisher, 2012:50). According to Braun and Clarke (2013:31) knowledge is the product of how the society comes to know and to understand the world; it can be either through manmade knowledge in form of ideological, political, cultural, moral or social, cultural contexts.

The research will explore a philosophical worldview to discover the meaning and understanding of the world in which the researcher works and lives on it, by analysis of the legal issues and challenges involved in virtual criminal investigations in Ghana. The belief is that trained security personnel such as Ghana police officers, National Security Officers can deliver real-time virtual policing and the reality of the cyber environment or virtual community expert good service delivery, the knowledge of the research is within the participant's experiences (Petersen &Gencel, 2013:2). The researcher will present the Anti-positivist (Phenomenologists, Interpretivists and Constructionist) and the Pragmatic worldviews as the worldviews adopted to support the research approach in this study.

1.7.1 PHENOMENOLOGISTS, INTERPRETIVISTS AND CONSTRUCTIONIST

1.7.1.1 Anti-positivist worldview

According to Welman et al (2012:6), the anti-positivists share the resistance to upholding the naturalistic-scientific methods as the norm in human behavioural research. According to anti-positivists, it is inappropriate to follow a strict natural scientific method when collecting and interpreting data. Anti-positivists believe that natural scientific methods are designed to study molecules or organisms and do not apply to the phenomenon being studied in human behavioural sciences Welman et al (2012:6). Mouton (2014:47) states that the anti-positivists believe that the differences between the social and natural world are so fundamental that there can be no basis for using the same methods and techniques in human science. Anti-positivist includes, inter alia, phenomenologists, Interpretivists and constructionist (Mouton, 2014:47). These anti-positivist approaches are discussed below.

1.7.1.2 Interpretivist

According to Anderson (2014:55) the word interpretivist means the researchers who are most comfortable with a socially constructed world view'. Interpretivists see the

information and facts as provisional and significantly affected by the meanings and experiences of different people in different situations of cultural contexts. Thanh and Thanh (2015:24) submit that the interpretive paradigm allows researchers to view the world through the perceptions and experiences of the participants. Furthermore, Thanh and Thanh (2015:24) state that in seeking answers for the research, the researcher who follows the interpretivist paradigm uses the experiences of participants to construct and interpret his/her understanding from the gathered data. Mason (2014:56) states that the distinctive factor about the interpretivist is that they see people and their interpretations, perceptions, meanings and understandings as the primary data sources. Interpretivist is concerned with understanding the social world people have produced and which they reproduce through their continuing activities (Mason, 2014:56). Anderson (2014:55) further indicates that the interpretivists are concerned with accessing and understanding the individual's perceptions of the world, they see social phenomenon (facts) as being products of human interactions. From the interpretivist perspective, the information from observations and interviews in the form of words and meanings (qualitative rather than quantitative) is often seen to be more valuable for researchers (Anderson, 2014:55). The focus of interpretivist research is therefore not on facts and numbers but words, observations and meanings (Anderson, 2014:55). In conclusion, Thanh and Thanh (2015:260) says that interpretivist researchers seek methods that enable them to understand in depth the relationship between human beings and their environment and the part those people play in creating the social fabric of which they are part. As the researcher views the world through the perceptions and experiences of the participants and in seeking answers to the research questions this worldview is appropriate for this study and also it allows the researcher to use those experiences to construct and interpret his understanding from the data gathered through interviews and observations.

1.7.1.3 Constructionist view

Tavakoli (2012:99) states that constructivism is the ontological and epistemological views which disallow the existence of an external objective reality independent of an individual from which knowledge may be collected or gained. Marvasti (2004:5) and Tavakoli (2012:

99) submit that individuals construct knowledge and his/her experience through social interaction, the constructionists are concerned with how human interactions help to create social reality. Constructivists believe that as human beings, we do not find or discover knowledge so much as we construct or make it. Within a constructionist model, subjective interpretations are not a source of bias, instead, they are considered a piece of an empirical puzzle that helps us understand how people accomplish social reality (Marvasti, 2004:5). Silverman (2014:24-25) shares the same sentiments with Marvasti (2004:5) and states that constructionist's sensibilities provoke questions about:

(a) how social realities are produced, assembled and maintained rather than trying to get inside social realities,
(b) processes through which social realities are constructed and sustained.

The constructionist desire is to step back from reality and describe how it is socially brought into being, rather than trying to get into social reality (Silverman, 2014:24-25). The constructionist paradigm represents a change from the focus on explaining phenomena typical in natural science to an emphasis on understanding, which is deemed appropriate for investigating phenomena in human science (Tavakoli, 2012:99). The constructionists are more concerned with the work or practices that go into creating the social world and less in its causes (Marvasti, 2004:5). Silverman (2014:26) further states that the important insight of constructionism is the realisation that facts are socially constructed in particular contexts, rather than to seek empathetic understanding of how people see things, it is concerned with questions of what and how. Constructionism is a theoretical position shared by many varieties of qualitative research including grounded theory, narrative and discourse analysis. Creswell (2014:8) submits that social constructivists believe that individual seeks an understanding of the world in which they live and work. Individuals develop varied and multiple subjective meanings of their experiences leading the researcher to look for the complexity of views rather than narrowing meanings into a few categories or ideas. The goal of the research is to rely as much as possible on the participants' views of the situation being studied. Tavakoli

(2012:99) concludes by saying that in terms of the methods, constructivist qualitative research studies typically emphasise participant observation and interviewing for generating data as the researcher aims to understand a phenomenon from the perspectives of those experiencing it. This study intends to explore virtual or cyber-criminal investigations in Ghana and its legal issues and challenges and make sense of the world that the participants work in, understand the participants' view about the cyber or virtual environment and understand the historical and cultural settings of the participants. This worldview is appropriate and applicable to this study.

1.7.1.4 Pragmatic worldview

According to Mouton (2014:8), the term "pragmatic" is derived from the Greek word 'prag-mein' and 'pragma' (thing or fact) which literally means to do. It has the same roots as 'practice' and 'practical'. The emphasis is on what is done, on outcomes rather than ideas or ideals. Bless et al (2015:16) state that the pragmatic worldview adopts the position that while human beings cannot be completely objective in their study of themselves and their world, it is nevertheless possible to develop shared knowledge that is useful in understanding our world and solving the problems that our communities face. This view combines a qualitative and quantitative approach to develop knowledge about the world that can be used to improve quality of life. Denscombe (2010:148) explains that a pragmatic worldview provides a set of assumptions about knowledge and inquiry and is regarded as the partner for mixed methods approaches as it underpins mixed methods approaches and distinguishes the methods from quantitative and qualitative approaches. Furthermore, Denscombe (2010:148) indicates that pragmatism revolves around the following ideas:

(a) Knowledge is based on practical outcomes and what works;
(b) Research should test what works through empirical enquiry;
(c) There is no single, best scientific method that can lead the way to indisputable knowledge;

(d) Knowledge is provisional, what we understand as truth today may not be seen as such in the future; and
(e) Traditional dualism in the field of philosophy and science is regarded as not helpful.

Pragmatism leaves the door open for the use of purely quantitative or purely qualitative research. Providing the use of either in isolation can produce the findings that work sufficiently well to answer a research problem (Denscombe, 2010:149). The pragmatic worldview does not necessitate the researcher to commit to any one system of philosophy and reality. The pragmatic worldview provides the researchers with the freedom of choice and allows the researcher to choose the most appropriate method for data collection and techniques for data analysis to address the research problem and answer the research questions. This philosophy is appropriate for this study as it allows the researcher to choose the methods, techniques and procedures that best suit the research needs and purposes.

1.8 RESEARCH APPROACH AND DESIGN

1.8.1 Qualitative Research Approach

The research approach is the plan and procedure to conduct research and it involves the connection of philosophy, research designs, and specific methods (Creswell 2014:3). According to Thomas (2013:104), the research approach is not just about whether you use this research method or that one, but rather is about how you think about the social world. Creswell (2014:3) mentions that the selection of the research approach is based on the nature of the research problem, the researcher's personal experience and the study audience. Researchers need to think through the philosophical worldview assumptions they bring to the study, the research design that is related to this world view and the specific methods or procedures of research that translate the approach into practice (Creswell, 2014:5).

The researcher followed a qualitative research approach and is of opinion that qualitative research provides answers to the research questions in this study. Schumacher and McMillan (2013:389) analyze and clarify that participant observation, in-depth interviews and artefact collection are the available strategies found in the qualitative approach. This study does not focus on data through questionnaires, systematic data analysis, observations and interviews. The study relies mostly on library materials, which include reports, legislation, court cases, regulations, charters, policies, amendments to legislation, academic journals, constitution, and textbooks. When using qualitative research, the researcher concentrates on spontaneously emerging languages and meanings. Many of these elements are directly observable and as such may be viewed as measurable data. Nonetheless, certain elements of symbolism, meaning, or understanding usually require consideration of the individual's perceptions and subjective apprehensions (Berg with Lune, 2012:15).

Qualitative approach takes the context of the study into account and this strengthens the validity of measures (Bless et al 2015:16). Anderson (2014:207) states that qualitative data helps the researcher to understand the issues in their organisational context and can enable the researcher to develop a 'rich picture' of processes that are taking place. According to Berg and Lune (2012:3), quality refers to the what, how, when, where, and why of things, its essence and ambience. Qualitative research thus refers to the meanings, concepts, definitions, characteristics, metaphors, symbols and descriptions of things. Welman et al (2012:188) describe qualitative research as an approach covering an array of interpretive techniques which seek to describe, decode, translate, and otherwise come to terms with the meaning of naturally occurring phenomenon in the social world.

1.8.2 Research Design

Creswell (2014:12) opines that after selecting the type of approach or method of study to conduct, the researcher must also decide on the type of study design. Lune et al (2010:76) are of the view that research design is the detailed plan that specifies the kind of data needed (measurement), the strategy for collecting the data (the research methods), the subjects (sampling) and the research site (when and where to get the data). The research design is where the researcher defines the scope of the research, the limits and the content of the data investigated. Babbie and Mouton (2012:74) agree with Lune et al (2010:76) and indicate that a research design is a plan or a blueprint of how the researcher intends to conduct the research, the research design focuses on the end product, the kind of study planned, and the results aimed at. Berg and Lune (2012: 96) submits that during the research design stage, the researcher can safely consider the actions that can be taken to the identities of the subjects and the data once it is collected, used and stored. Astalin (2013:119) states that the four major types of qualitative research designs are: “Phenomenology; ethnography; grounded theory and case study. In this study, the researcher employed a case study. The case study is a strategy of inquiry in which the researcher explores in-depth programmes, persons, events, decisions, activities, periods, projects, policies, institutions or other systems that are studied holistically by one or more methods” (Astalin, 2013:122; Creswell, 2009:13).

1.9 METHODOLOGICAL FRAMEWORK OF THE STUDY

Seale (2004:13-14) posits that methodology involves presenting rules of procedure about matters such as the collection of data and their analysis. Berg and Lune (2012:400-401) agree with Seale (2004:13-14) and submit that the purpose of the methodological section is to explain to the readers how the research was accomplished; what the data consist of and how data were collected, organised and analysed. Babbie and Mouton (2012:49) state that the words methodological paradigm and methodological approaches are interchangeably used. Furthermore, Babbie with Mouton, (2012:49) states that methodological paradigms are more than a mere collection of research methods and techniques, the word is used to include both the actual methods and techniques that

social researchers use as well as the underlying principles and assumptions regarding their use.

Berg and Lune (2012:401) state that explaining the details about how the research was conducted is like telling a story and the points of detail most important to the researcher may vary from study to study. According to Marshall and Rossman (2016:6) “conceptual frame must be linked to existing puzzles” and Ravitch and Riggan (2012:10) also state that conceptual frame can be viewed as an epistemology stance, as the researcher can use assumptions and beliefs to construct quality knowledge, on how the researcher problem can be explored; the question based on the nature of knowledge required for the study will be, how knowledge can be acquired. Therefore conceptual frame can be asserted as the starting point of the study (Kumar, 2014:57). Silverman (2014:54) shares the same sentiments with Berg and Lune (2012:401) and states that methodology refers to the choices that the researcher makes about the cases to study, methods of data gathering, and forms of data analysis in planning and execution of the research. Anderson (2014:52) states that the term methodology refers to the theory and philosophy of how research should be undertaken. Khaldi (2017:16) submits that the type of research methodology the researcher chooses is determined by the research philosophy to which the researcher adheres and this choice will determine the research objectives, and the research instruments developed and used as well as the quest for a solution to the problem researched. Furthermore, Anderson (2014:52) states that philosophy is concerned with how as thinking human beings, we make sense of the observable world, it is concerned with the fundamental nature of knowledge.

1.9.1 Research Methods (Data Collection)

To begin with, it must be considered that the outermost in this study methodology is conceded as a scientific discipline and doctrinal legal discipline in implying mounting out and defining the most appropriate ways of having or showing good judgement in the subject of investigation in the study. In this study, legal methodology (Vibhute and Aynalem, 2009) is used to discern law and legal phenomena of cybercrime investigations

through analysis of statutory provisions and cases by application of power of reasoning and give emphasis on analysis of legal rules, principles and doctrines. The methods denote a range of approaches used to gather data, which are to be used as a basis for inference and interpretation, for explanation and prediction.

Thus, methods are in essence of data collection or data gathering (Sibanda, 2015:59) claimed that legal study must be undertaken from the perspective of social science and the fact that it is very appropriate to elicit the relevant information for the study. In this respect, the criminal justice and investigation research methods approach was applied in the field of law in this study which will be empirical in nature. Empirical studies generate data from observation and experience (Maxfield & Babbie, 2014:258). This choice was made based on the criticisms of the black letter approach or methodology of legal research. Nkansah and Chimbwanda (2016:55) recounted some of these processes as legal claims-making, the use of legal authorities; and analytical reasoning. The interdisciplinary approach has been accepted as an important mix of other fields to that of law for legal knowledge acquisition by modern legal scholars (Nkansah & Chimbwanda, 2016:55). Below are the data collection methods used in this study:

1.9.2 Literature Review and Document Analysis

Maree (2011:102) states that “data gathering technique such as a document is a written communication that may gravitate or make it possible to understand or know more about on the phenomenon researched". Document analysis and literature review are distinct from one another. Review of literature involves published documents, such as books and journal articles, whereas documents may include government documents and minutes written by co-operations and they are not published but may provide valuable information about the study to the researcher.

According to Creswell (2015:25), conducting a literature review is to share the results of other studies that are similar to the study being undertaken, to provide a framework for establishing the importance of the study undertaken, and to provide a benchmark for comparing the results of the study with other findings. According to Kelly (2016:316),

documentary sources are sources such as letters, newspaper articles, official documents and books. Babbie and Mouton (2012:300) indicate that personal documents such as diaries, letters, photos, memos, biographies, graffiti, suicide notes, etc. share the essential elements of human or personal characteristics of the author of the document. The author of the document expresses him/herself in the document and when reading the document, the reader of the document comes to know the author and his/her views of events with which the document is concerned.

Adler and Clark (2011:89) state that literature review is the process of searching for, reading, summarising and synthesising existing work on a topic or the resulting written summary of a search. According to Berg and Lune (2012:26) and Thomas (2013:58) are of opinion that after the researcher has outlined the problem or issue to be examined and expressed in the form of a research question, the next step is to find out what other people have accomplished in researching the topic under study. The researcher needs to begin examining how others have thought about the researched topic by going to the library and conducting a literature review. According to Bless et al (2015:21), the purpose of reviewing the literature is to increase the researcher's understanding of the concept under investigation and for the researcher to learn first-hand what has been studied on the specific question/topic.

For data collection in this research, a literature review was conducted in the fields of cybercrime Investigations, digital forensics, digital evidence, search and seize, admissibility of digital evidence, digital crime, criminal procedure, prevention and deterrence, forensic analysis, court proceedings, legislations, digital prosecutions, policing on the internet and other related subjects. Badenhorst (2014:43) advises that a literature review is not the summary of what exists in the literature, but it is the representation of the literature with evidence drawn from articles and books to provide strengths to the claims being made. The literature review contains claims of what exists in the literature. Leedy and Ormrod (2013:51) reveal that the role of the literature review is to look again at what others have done in areas that are similar, though not necessarily

identical to one's topic of investigation. Fouche and Delport (in De Vos et al. 2011:34) and Creswell (2014:36) point out the following steps when collecting literature in a study:

(a) Finding appropriate literature/Data Location: The topic for the research is determined, studied, and analysed to find literature which is similar to the problem. Key concepts such as cybercrime, digital forensics, investigations, digital evidence, cybercriminal, prosecutions, chain of custody, search and seizure, legislation, and court cases will be identified by the researcher to set out the topic and research questions in the study. The distinct concepts of the topic and in addition the keywords of the research question are used to search the electronic databases of the Cybercrime Unit of Ghana Police, the Ghana Ministry of Justice, the United States National Institute of Justice, the US Federal Bureau of Investigations (FBI), Australia National Institute of Justice, United Kingdom National Crime Agency (NCA), the European Union Agency for Law Enforcement Agency better know under the name Europol, the International Criminal Police Organisation commonly called Interpol and University of South Africa (Unisa) library for journals, books, research reports, short dissertations, dissertations and theses related to the topic.

In addition, the researcher searches the online platform of the Texas Department of Criminal Justice and United States Department of Justice online repository to conduct a literature search. The researcher searches the online computerised databases of Unisa library websites that are most regularly reviewed by social science researchers, such as Google Scholar, ProQuest, the Social Science Citation Index and others. The researcher also uses the internet to find material relating to this research.

(b) Document Selection**:** Selection of documents by the researcher is one of the key areas in conducting research. The researcher scrutinizes, reads and looks through all the pertinent literature obtained, and the literature directly related and central to the researcher's study is duplicated for further study. During this process, the researcher repeatedly aspires to obtain awareness of indicating the most appropriate and relevant that will make a useful contribution to the topic under study. Thus a literature map is compiled by the researcher throughout the process of identifying relevant literature to provide a visual pictorial that demonstrates how the study position into the larger body of the literature gathered through the literature review process. The researcher compiled and sum up the relevant literature that is discussed in the relevant chapters of the study are listed in the list of references

(c) Document analysis: The researcher analysed the documents found and selected as indicated above. The selected documents for the analysis include materials obtained through court records, or case law reports, forensic investigation reports, government cybercrime policy documents, cybercrime newspapers, local and international articles on cyber security and cybercrimes, crime scene investigations, and also academic documents such as journal articles on criminal procedures, digital evidence admissibility, conference papers and books on cybercrime investigations.

1.10 RESEARCH PARADIGM

Creswell (2015) highlights that research paradigm is a set of ideologies and presuppositions that guide the researchers on how to triumphantly execute their studies. In this case, Creswell and Plano (2017:67) observed that the research paradigm is intended to guide the inquiry in this study. With the many understanding of research

paradigms in existence, Sibanda (2015:51) explicated that it is not surprising when each researcher "approaches research with a plethora of interlocking and sometimes contradicting philosophical assumptions and stances.The following research paradigms are used to analyse and interpret available data to answer research questions or phenomena in this study:

1.10.1 Comparative Paradigm

As claimed by Fombad (2017:984) comparative legal research, as a research paradigm "is of such critical importance to legal research" and it defies logic why it is not part of the design of African university's legal research studies. Fombad (2017:985, argues that all legal research involves, directly or indirectly, some degree of comparison and it is indispensable that legal studies or legal research apply certain principles and methodologies of comparative law. The comparative legal research methodology was used in this study focusing on selected national jurisdictions and international frameworks for cybercrime investigations. Van Hoecke (2011) claimed that comparative evaluation is used with regard to carefully selected comparator jurisdiction, namely, the United States of America (USA), United Kingdom (UK), Australia, and South Africa (SA), to ascertain how their anti-cybercrimes systems tend to be different with Ghana in the eradication or combating cyber-criminals. In addition, comparative research assists the researcher to find out, if any valuable lessons can be learned from their standard frameworks and the performance of their anti-cybercrime agencies. One important consideration that was highlighted by Fombad (2017:991) is that comparative legal research is a key to any research aimed at drafting harmonised laws or drawing up international conventions and agreements. Since there have been legislative changes in Ghana on the anti-cybercrime framework, a comparative research approach is important in the context of this study.

1.10.2 Critical Paradigm

As the title of the study postulates, the essence of this study is "An exploration of cybercrime investigations in Ghana" from a comparative study approach. Given this, a

critical paradigm is used to achieve the objective of this study which involves an analysis of investigating all the legislative frameworks of cybercrimes and its prosecutorial or investigations agencies or institutions in Ghana. Consequently, critical discourse analysis is employed (Asghar, 2013:3124) in this study to allow the analytical and critical nature of the study, and also to expose and challenge the inefficiencies of dealing with cybercrime in Ghana.

1.10.3 Interpretive and Descriptive Paradigm

In this study, the research paradigm is interpretive. The study for the most part focuses on expounding or interpreting existing laws, pieces of legislation and judgements, observing and analyzing the implementation of the existing cybercrime framework and policies, and also interpreting observations, and views that are found on the subject from the review of the literature. On the subject of descriptive paradigm, the researcher provides a descriptive analysis of the inefficient of cybercrime investigative strategies in Ghana, the lack of combined action between the various cybercrime investigations agency strategies in the government of Ghana and the lack of interlinkage between these anti-cybercrime strategies and various government departments which bring negative impact on non-compliance and adherence to policy. Intending to produce that result, the research put together, evaluate and wrote down all information to the group and classify to find and promote the body of knowledge in this field of study. Using the information, data and knowledge gained throughout this study, the researcher points out relationships and relatedness across governmental departments to build possible relationships to deal with the cybercrime canker in both public and private cooperation and institutions.

1.11 RESEARCH DEMARCATION AND LIMITATIONS

Goddard and Melville (2004:14), indicate that the process of demarcation specifically involves researchers determining the scope of the study; what variables are involved; how the study will be conducted; and what practical constraints or challenges will be experienced. According to Denscombe (2010:69), the term delimitations means to demarcate, or to set boundaries around something, delimitations involve setting limits and

are the self-imposed boundaries by the researcher" that are concerned with specifying things such as:

(a) The boundaries to the literature that will be reviewed;
(b) The items or people that will be included in the research and those that will not and why;
(c) Factors that will be looked at in the research and those that will not and why; and the period to be covered.

Leedy and Ormrod (2014:43) share the same sentiments as Denscombe (2010:69) when they indicate that what the researcher does not intend to do is stated in the delimitations. It is important to know precisely what the researcher does not intend to do. The following are the delimitations of this thesis:

(a) The Ghana criminal justice system consists of many pieces of legislation dealing with specific areas of criminal activities, some mutually exclusive and others mutually inter-dependent. An academic study like this may not cover all this legislation. Thus in this study, only a selected band of legislation is considered, namely: Electronic Transaction Act, 2008 (Act 772), Electronic Communication Act, 2008 (Act 775), Data Protection Act, 2012 (Act 845), Criminal Offence Act, 1990 (Act 29), Criminal Offences Procedure Act, 1960 (Act, 30). However, not all of this selected legislation is dealt with in depth for this study. Some are already addressed generally elsewhere in some major studies.

(b) Several institutions are referred to as relevant to the broader scheme of fighting cybercrime. These are, for example, the Ghana Police Service, National Security, National Intelligence Bureau, Ghana Commission of Human Rights and Administrative Justice (CHRAJ),

Office of Special Prosecutor, Parliamentary Committee on Communications, Ministry of Communications, National Communication Authority, and the several law enforcement divisions. Some of these institutions such as the “CHRAJ” are not dedicated specifically or primarily to fighting cybercrime or virtual criminality in general and they will thus not be discussed extensively.

(c) Several digital evidence collection and Search and Seize methodologies and applications that have been introduced in the understudy countries and are relevant to this research will be dealt with. But evidence collection that does not have a clear understanding will not be focused on.

1.12 VALIDITY AND RELIABILITY

Each study draws strength from the validity, accuracy and reliability of its findings. “In Creswell’s view (2014:210), validity and reliability of the research must not only be accurate from the perspective of the researcher but also must be exact from the reader of an account and the participants. Mouton (2014:108) posits that the rationale of the research design is to plan for and structure the research project in such a way that the validity of the research findings is maximised through either minimising or, where possible, eliminating potential errors. Bless et al (2015:131) also mention that in quantitative research, internal validity is concerned with the question whereas, in qualitative research, internal validity sometimes refers to credibility and relates to ascertaining whether the data collection methods and analysis adequately answer the research question. Furthermore, these authors, Bless *et al* (2015:131) state that research design is the specification of the most adequate operations to be performed to test the specific hypothesis under given conditions and requires a thought-out strategy.” Validity and reliability in this study were secured through the following strategies/approaches:

a) Supplication of critical expert peer-review of the study or parts of the study

b) Avoid bias as far as possible. Cohen, Manion and Morrison (2017:165) describe bias as a "systematic or insistent tendency to make errors in the same direction, that is, to overstate or understate the true value of an attribute." In this study, self-reflection created an open and honest narrative and should resonate well with readers. Because of this, the researcher indicated the cybercrime training he had with E-crime Bureau and Ghana Police Services and also his research interactions and criminal justice conferences he attended with academic professors, professional investigations experts, cybercrime lawyers, cybercrime police officers in the United States, Australia United Kingdom and South Africa where he gained first-hand information on the cybersecurity regulatory and institutional framework in the country under study. This experience has partly influenced the researcher's election of the countries under study and qualitative research contains comments by the researcher about how their interpretation of the findings is shaped by their institutional systems.

1.13 VALUE OF THE RESEARCH

De Vos *et al*., (2011:107) and Denscombe (2010:24) are of the opinion that research must be able to be used for practical purposes, should be useful to the intended target group and must contribute to the generation of new knowledge. In this study, it is thus expected that in:

a) **Academia** – the findings of this research will contribute to the body of knowledge of virtual crime from a developing country perspective and it could also encourage others to do further research in that area of study.

b) **Government** – to the government, this research shall provide a means of assessing the progress of laws for combating virtual crime and the strides that law enforcement has made so far, and also identify the challenges it is facing. It could also help in formulating policies to modernise the incident response team for the virtual crime.

c) **Financial Institutions** – the new millennium has brought with it a new financial landscape, one filled with emerging technology, new applications and opportunities which has led to changes in customers' lifestyles and demands leading to a new anytime, anywhere attitude to banking and financial services. The industry's demand for more secure, low-cost transactions and new value-added services has therefore fuelled mass migration towards a microprocessor-based e-payment and smart card technology and because it has been proven to reduce fraud, it has created a new route for fast adoption by the developing (countries) market. This research shall therefore portray the benefits and problems associated with technology and enable the industry to become more competitive by formulating policies to streamline its operational security.

d) **Public** – this research shall serve as a means of increasing and educating the public on the need to be abreast with the law on cybercrime to help the economy move in accordance with technological changes going on in the world.

e) **Students and other Researchers**– this research shall also serve as a foundation for them when undertaking similar studies to unearth new ideas for future research and finally to add to the existing limited body of information on cybercrime and the law available in Ghana.

1.14 CLARIFICATION OF KEY TERMS AND CONCEPTS

According to Bless *et al* (2014:80), verbal communication among human beings would be impossible without the existence of words expressing concepts. According to De Vos *et al*., (2011:32) “definitions are used to facilitate communication and arguments”, particularly because they present terms and/or concepts simply and clearly, thus avoiding vagueness or ambiguity. Defining terms focuses the researcher (Maxfield with Babbie,

2014:20). Bless *et al* (2014:50) state that for concepts to be useful they must be defined in a clear, precise, non-ambiguous and agreed-upon way. Leedy and Ormrod (2014:43) support this statement and emphasized that in defining a term, the researcher makes the term mean whatever he or she wishes it to mean within the context of the problem and its sub-problem and that other individual who read the report must know how the researcher defines the term and understand certain concepts and be able to appraise the report or research appropriately. The following are the concepts and definitions that form part of this research and discussions;

1.14.1 Virtual Crime

Osterburg and Ward (2010:303) define crime as an act committed or omitted in violation of a law forbidding or commanding it, and for which punishment is imposed upon conviction. Mohamed, Ashraf, and Khan (2015: 58) posit that cybercrime or Virtual crime or "e-crime" or "computer-related crime" "digital technology crime" is a long-established phenomenon. Any criminal activity that involves a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of virtual crime or cyber crime

1.14.2 Criminal Investigation

Karen, Christine and Henry (2017:9) state that criminal investigation is the process of discovering, collecting, preparing, identifying, and presenting evidence to determine what happened and who is responsible. The criminal investigation is a reconstruction process that uses deductive reasoning, a logical process in which a conclusion follows from specific facts (Karen, Christine & Henry, 2017:9)

1.14.3 Computer Forensic

EC-Council (2017: 123) states that computer forensics is the preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, the integrity of evidence, factual reporting of information

found, and providing expert opinion in a court of law or other legal and or administrative proceeding as to what was found. Computer forensics can be referred back to as early as 1984 when the FBI created the Magnetic Media Program, which initially only handled three cases in its first year. The magnetic media program later becomes the FBI Computer Analysis and Response Team (CART) program. At the end of 2009, the FBI had fourteen Regional Computer Forensic Labs (RCLs) in operation. As technology has progressed, the field of computer forensics has been forced to expand to cover other types of electronic data, created by a myriad of devices.

1.14.4 Digital Evidence

André (2018: 151) claimed that central to any digital investigation is the notion of digital evidence. Digital evidence is defined as any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi. Casey (2011: 186) also claimed that digital evidence is any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrators.

1.14.5 Digital Crime Scene

Crime scene processing is an inherent task and duty associated with most criminal investigations, for rarely does one encounter a crime without some kind of crime scene. Crime scene investigation is more than the processing or documentation of crime scenes, nor is it just the collection or packaging of physical evidence (Eoghan, 2011:227). Computers, mobile devices, and networks should be considered an extension of the crime scene, even when they are not directly involved in facilitating the crime, as they can contain useful information and provide a digital dimension (Eoghan, 2011:56). Like a physical crime scene, the digital crime scene can contain many pieces of evidence and it is necessary to apply forensic principles to survey, preserve, and document the entire scene.

1.14.6 Chain of Custody

Andre (2018:06) affirms that chain of custody refers to the documentation of acquisition, control analysis, and disposition of physical and electronic evidence. The chain of custody form should include: the case number, nature of the case, an investigator for the case, evidence recorded, date and time, the location from which the evidence was recovered, evidence processed by item number, and investigation organisation.

1.14.7 Admissibility

To Eoghan (2011:56) the concept of admissibility is a simple one. Court need to determine whether evidence is "safe" to put before a jury and will help provide a solid foundation for deciding the case Eoghan (2011:56). Eoghan (2011:56) indicated that admissibility is a set of legal tests carried out by a judge to assess an item of evidence. This assessment process can become complicated, particularly when the evidence was not handled properly or has traits that make it less reliable or more prejudicial. Some jurisdictions have rules relating to admissibility that are formal and sometimes inflexible while other jurisdictions give judges more discretion (Eoghan, 2011:56).

1.15 ETHICAL REVIEW

As a rule of practise, the researcher was required to comply with ethical principles as provided for in UNISA's policy on research ethics of 2016. The researcher follows the UNISA research ethics while conducting his research and obtained ethical clearance from the ethical clearance committee of the UNISA, College of Law. The study was also submitted to the Turnitin software to check and confirm the academic integrity of the study, and similarity index that is attached at the end of this document. Anderson (2014:149) concludes by saying that research ethics is about adherence to a code of behaviour in relation to the rights of those who become the subject of research or are affected by it. Explicit concern with ethical issues is a fundamental feature of good research.

1.16 RESEARCH STRUCTURE

- **CHAPTER ONE: GENERAL ORIENTATION**

This chapter focuses on the discussions on the introduction, rationale of the research, aim, purpose and objectives of the research. The research questions; key concepts delimitations of the study as well as the literature review are also discussed in this chapter.

- **CHAPTER TWO: VIRTUAL CRIMES**

This chapter focuses on the contextual overview of Virtual Crimes: Internet Vulnerabilities and criminal activity, classification of virtual criminal activities against persons, property, government, and Society.

- **CHAPTER THREE: COMPUTER FORENSICS AND VIRTUAL DETECTIVE WORK**

In this chapter, the research explored computer forensics and its sub-disciplines. Legal issues and investigative procedures, virtual criminal investigation approaches and challenges, cybercrime unit of the Ghana police, South Africa electronic crime unit, Australia high tech crime centre, US department of justice cybercrime section, UK national cybercrime unit and comparative analysis will be studied. Also, this chapter focuses on virtual crime scenes, photographs, videography and investigation models of the countries under study. Comparative legal analysis will be done among the countries. Virtual criminal investigation challenges, legal issues, privacy and jurisdictional issues in virtual forensic investigations will be studied.

- **CHAPTER FOUR: SEARCH AND SEIZURE OF VIRTUAL EVIDENCE**

This chapter direct the search and seizure of digital evidence and the approaches used by the countries under study. Issues such as reasonable grounds, subject of the search

warrant, scope of the search warrant, search location, searching and seizing without a warrant, exceptions that allow searching and seizing without a warrant, consent searches and its scope, the plain view doctrine and incident to a lawful arrest, privacy issues during search and seizure and comparative analysis of the countries under study were explored.

- **CHAPTER FIVE: VIRTUAL EVIDENCE, ADMISSIBILITY AND EVIDENTIAL WEIGHT**

In this chapter virtual evidence perspective in terms of admissibility and evidential weight were explored. The type of virtual evidence on digital devices were studied, authentication of virtual evidence in criminal and civil proceedings, rules of admissibility for virtual evidence, weight, credibility and sufficiency of virtual evidence, the role of judges in evaluating virtual evidence, judge's role in admitting virtual evidence, legal issues on the admissibility of virtual evidence in Ghana, United States, Australia, United Kingdom, South Africa, were studied. The chapter concluded with a comparative legal analysis of the countries under study.

CHAPTER SIX: RESEARCH FINDINGS, CONCLUSIONS AND RECOMMENDATION.

A comparative determination and appraisal of the Ghana anti-cybercrime strategies and structures is undertaken in this thesis. In particular, the thesis focuses on the efficacy on the anti-cybercrime agencies, and other virtual criminal investigators and the role they play in combating virtual crime or cybercrime in Ghana. This chapter contains a general conclusions and research findings from data obtained from both literature review and qualitative research. The chapter makes a number of important submissions and recommendations for consideration by the Ghanaian authorities. Provisions for recommended constitutional and legislative reforms are suggested where possible

1.17 CHAPTER SUMMARY

This chapter presented the introduction where the researcher introduces the readers to the topic, the background, and where the cost of cybercrime in Ghana is discussed in detail, including the lack of investigation skills by law enforcement and insufficient laws to prosecute cybercriminals. The problem statement of this study is discussed, the research

aims and objectives are highlighted, the key concepts are defined and how the data was collected and analysed was also discussed and the value of the study is explained briefly.

CHAPTER TWO

RUDIMENTARY OVERVIEW OF VIRTUAL CRIMES

2.1 INTRODUCTION

The objective of this chapter is to give e rudimentary overview of the most common types of virtual crimes and the response of the legal fraternity to these crimes. It is important for law enforcement agencies, especially the computer crimes units or the cybercrime units to have an in-depth understanding and the ability to establish the various types of virtual crimes and the differences between them as well as the legal response to them. Given the legal issues involved and the complexity of the criminalisation of virtual crimes is necessary for law enforcement personnel to respond to and build effectively at local, National and international levels, a strategy against virtual crime. One of the pivotal events in human history is the invention of the computer, alongside other significant and prominent developments experienced by human beings in the late eighteenth and early nineteenth centuries. The dawn of virtual or internet-based information systems and technology has witnessed an emergence of a revolutionised transformation in the form of

advancement and development of civilized society. The advancements made by modern technology have facilitated communities to develop and expand their communication networks thus enabling faster and easier networking along with information exchange. Cyber technology has become an essential part of our day-to-day life. With the expansion of the use of virtual or cyber technology in almost every sphere of human life, there is virtually no room left for us to think of a life without the centrality of technology. According to the United Nations Office on Drugs and Crime (UNODC) 2020 internet tools have been integrated into the business models of traffickers at every stage of the process. The Interconnected network has become part of the process of globalisation that is displacing former realities and certainties, creating new opportunities and difficulties associated with living in a 'shrinking' world. UNODC in 2013 posited that developing countries constitute 60 per cent of all internet users with 45 per cent of all internet users below the age of 25 years. UNODC further noted that in the hyper-connected world it would become hard to imagine a ‘computer crime’, and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity. In many countries, the explosion in global connectivity has come at a time of economic and demographic transformations, with rising income disparities, tightened private sector spending, and reduced financial liquidity (UNODC) 2013). At the global level, law enforcement authorities perceive the increasing levels of virtual crime, as both individuals and organized criminal groups exploiting new criminal opportunities, driven by profit and personal gain. The recognition and enthusiasm for these changes have been tempered by fears that the Internet brings with it new threats and dangers to our societal security.

2.2 DEFINING VIRTUAL CRIMES, INTERNET VULNERABILITIES AND CRIMINAL ACTIVITIES

Legal implications of virtual crimes require, first, the definition of those actions that surround internet-based information technology which in one way or the other may cause harm and lastly the criminalization of those actions. Therefore, both the strength and weaknesses of these laws, namely: the Ghanaian Criminal Code, the Electronic Transaction Act, the Electronic Communication Act, the Data Protection Act and the

National Information Technology Agency Act will be examined in addressing different aspects of virtual crimes.

To clearly understand the meaning of Virtual Crime, one should first understand the meaning of the term Crime and then the meaning of Virtual Crime. Madzivhandila (2019) has argued that crime is a social problem in society and it affects thousands of people every year and casts fear whiles restricting people's freedom of movement and preventing them from participating wholeheartedly in community activities. Crime is not per se a legal term. It derives its meaning and has a connotation in the background of a society than the State as such. Thus, it defies an attempt to lay down a straight jacket definition with clearly defined boundaries. However, usually, it is put synonymous with something which is "a wrong", "an offence", "a misdemeanour" or "a felony" “(The Institute of Company Secretaries of India), 2016).” Crime is as old and historical as human society itself. Many ancient books, right from the pre-historic days, and mythological stories have spoken about crimes being committed by individuals; be it committed against an individual like ordinary theft and burglary or the nation at large like the crimes of spying, treason, etc. According to Merriam-Webster Dictionary (2022), crime is an act or the commission of an act that is forbidden or the omission of a duty that is commanded by public law and that makes the offender liable to punishment by that law, especially - a gross violation of the law. Oxford English Dictionary on the other hand also defines crime as an action or activity or omission considered to be evil, shameful, or wrong; which constitutes an offence and is punishable by law. In layman's language, a crime can be defined as an unlawful act punishable by a State or other authority. The term "crime" does not, under modern criminal law, have a simple and universally accepted definition, though statutory definitions have been provided for certain purposes. The most popular view is that crime is a category created by law; in other words, something is a crime if it is declared as such by the relevant and applicable law. One definition is that a crime or an Offence (or criminal offence) and an act harmful not only to an individual or individuals but also to the community, society or the State at large (" a public wrong").

Deducing from the definitions of the term ‘Crime’ above, Virtual crime can be defined as an act or omission prohibited by law which is carried out either with the means of or where

the target is a computer, computer source or computer network (Institute of company secretaries of India, 2016). There are, at present, a large number of terms, definitions and taxonomies proposed or used to describe crime involving computers. These terms include Virtual crime, computer-related crime, computer crime, Internet crime, e-crime, digital crime, technology crime, high-tech crime, online crime, electronic crime, computer misuse, and cybercrime. Virtual crime or cybercrime is necessary to delineate the outer limits of the subjects of study and to distinguish it from other or real-world crime and offensive information operations. Consequently, it is noted that a wide range of differences at the international level usually makes it impossible to reach a complete accord definition of a controversial phenomenon. For instance, the definition of terrorism by the international community has not been reached meanwhile more than a hundred scholarly definitions of terrorism have been put forward. Similarly, while virtual crime or cybercrime is widely considered a new evolution of crime compared with older real-world crimes, there is no internationally unanimous definition.

The principal obstacle to reaching a comprehensive definition of virtual crime or cybercrime is that internet based-information systems keep evolving and therefore allow ever more innovative crimes to be committed in cyberspace. Nevertheless, academics researching the emerging field of virtual crime studies have dedicated their effort to an exhaustive definition of cybercrime. They interchangeably used terms such as computer crimes, digital crimes, virtual crimes, electronic crimes, information highway crimes, cyber-crimes, high-tech crimes, computer abuse, computer fraud and internet crimes, all of which describe illegal activities taking place in cyberspace or associated with computer networks. Arguably, this legal jargon can be condensed into no more than three general headings namely "cybercrime, virtual crime or computer crime". As will be explained later, virtual crime and cybercrime or computer crime terminologies are interchangeably used in this research.

Virtual crimes are technology-based crimes wherein the computer or internet itself is used as a weapon or means to commit such crimes. According to Symantec Corporation (2020) virtual crime or cybercrime is "any crime that is committed using a computer or network,

or hardware device". This is a very broad definition that not only includes crimes that use or target computer systems and networks but also includes crimes that happen within a stand-alone hardware device or computer. Kshetri (2006:33) analyses virtual crime or cybercrime and its motivation in terms of cost-benefit to the cyber-criminal and defines cybercrime as a crime that utilizes a computer network during the committing of crimes such as online fraud, online money laundering, identity theft, and criminal uses of Internet communication. While some writers describe cyberspace and the new types of crime as "new wine, no bottles", however, in contrast, other scholars suggest that it is a matter of "old wine in new bottles", since cybercrime is "basically the same as the terrestrial crime with which we are familiar".

The term 'Virtual crime or cybercrime' involves not only new crimes against computer data and systems, but it also involves traditional crimes such as fraud. In 2009 the Council of Europe (CoE) classified cybercrime into four main categories: namely, offences against confidentiality, integrity and availability of computer systems and data; computer-related offences (forgery, fraud); content-related offences; and offences related to infringements of copyright and related rights. However, Alkaabi, Mohay,Mccullayh and Chantler (2010:3) contend that the CoE cybercrime categorisation does not include some types of crimes that have been committed or facilitated using the computer such as money laundering, identity theft and storing illegal content. The United Nations (UN) manual on the prevention and control of computer-related crime, published in 1999, lists five common types of computer crime: fraud by computer manipulation; computer forgery; damage to or modification of computer data or programs; unauthorised access to computer systems and services; and unauthorised reproduction of legally protected computer programs. Though the UN manual includes crimes against computer data and systems, it also covers some crimes that utilize computer systems such as fraud and forgery. However, the manual does not refer to other types of offences that are committed or facilitated by a computer or computer system such as identity theft, money laundering and storing illegal content.

In 2007 the U.S. Department of Justice defined computer crimes or virtual crime as "crimes that use or target computer networks, which we interchangeably refer to as 'computer crime,' 'cybercrime,' and 'network crime'", and refers to viruses, worms and Denial-of-Service attacks. Also in 2007, the United Kingdom Association of Chief Police Officers (UKACPO) described e-crime as the "use of networked computers, telephony or Internet technology to commit or facilitate the commission of a crime", which is consistent with the original, network-specific, origins of the term cybercrime.

Brenner (2011:15) classifies cybercrime into three categories, namely: "the use of a computer as a target of criminal activity (e.g., hacking, dissemination of viruses and worms), the use of a computer as a tool or instrument used to commit a criminal activity (e.g., online fraud, harassment), and the use of a computer as incidental to the crime (e.g., data storage for a drug dealer to monitor sales and profits)" with the concurrence of some authors (Symantec Corporation, 2017; Viano, 2017, Donald and Kweku, 2014). Still, however, classify cybercrime into only two categories (Koenig 2002; Lewis 2004, Australian High Tech Crime Centre, 2013). Notably, the Foreign Affairs and International Trade of Canada (2006) classifies cybercrime into two categories, namely: a crime that is committed using computers and networks (examples hacking and computer viruses) and traditional crime that is facilitated with computers (example child pornography and online fraud). The crimes which cover the indirect use of computers by criminals (for example communication, document and data storage) are termed computer-supported crime and not cybercrime Foreign Affairs and International Trade of Canada 2006. Likewise, the categorization by Urbas and Choo (2008:28) identifies two main types of cybercrime: these are crimes where the computer is a target of an offence (for example, hacking, and terrorism) and crimes where a computer is a tool in the commission of the offence (e.g., online fraud, identity theft). Urbas and Choo (2008:28) elaborate on the second type, the computer as a tool, based upon the level of reliance on technology: computer-enabled crimes, and computer-enhanced and computer-supported crimes.

Information and communications technologies (ICTs) have exponentially grown in their agility for use and contributed to the growth of organized crimes and an illicit global economy (Etges with Sutcliffe, 2011:106). The porosity and anonymity of the Internet

have superimposed in a complex interaction that has enabled criminal and violent groups, transnational terrorist organizations, and companies engaged in espionage to expand their operations globally. There has been an indication that Government-backed cyberwarfare in some countries and maverick hackers testing their skills have further threatened the security of the digital world. According to SABRIC Annual Crime Statistics reported(2018) the combined gross card fraud losses on South African-issued cards saw an 18% increase from 2017 to 2018, totalling R873 394 351, with credit card fraud increasing by 18.4% and debit card fraud increasing by 17.5%. The statistics further add that 23466 incidents across banking apps, online banking and mobile banking amounted to R262 826 888 in gross losses.

It is concerning, however, that incidents across these platforms increased by 75.3%. Mobile banking incidents showed an increase of 100%, with gross losses of R28 941 040, while online banking incidents showed an increase of 37.5% with gross losses of R129 002 523 (South Africa Bank Risk Information Centre (SABRIC, 2018)**.** Banking app incidents increased by 55.4%, with gross losses of R104 883 325 for the same period. SIM swops in the Mobile Banking space saw an increase of over 200% to 11077 incidents (South Africa Bank Risk Information Centre (SABRIC) 2018)**.**

According to a report released by the FBI in January 2006, the agency tracked cyberattacks targeting the United States from 36 different countries (Regan, 2006). Commenting on a rapid rise of virtual crime or cybercrimes, McAfee analyst Greg Day note that Blackmail, money motivation and new opportunities cross international borders (Muncaster, 2006). Hi-tech and cybercrimes are among Interpol's top six priorities, namely drugs and criminal organizations, tracking fugitives, public safety and terrorism, trafficking of human beings, and corruption are the other five (Interpol annual report, 2007). Steffensmeier and Ulmer (2014) note that the concept of criminal entrepreneurship implies that some groups are better endowed to exploit opportunities for illegal gain, whereas other groups may be weakly positioned to do so.

Kshetri (2010) argues that considering the stereotypically different expectations that surround cyber-criminals, it is important to note that this new breed of criminals does not consist of isolated individuals working on home computers. Indeed, cybercriminals resemble criminals in the conventional world. In 2019 Ghana lost $ 105million and 9.8 million in 2018 due to internet fraud and cybercrime (Ghana Computer Emergence Response Team 2021). As of September 2021, the Cybercrime Unit of the Criminal Investigations Department (CID) of the Ghana Police Service said cyber frauds represented 45% of all cybercrime cases, making it the topmost. Cybersecurity Ventures also predict that global cybercrime cost to grow by 15 percent per year over the next five years, reaching $ 10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015 (Cybersecurity ventures, 2021).

The effects of the expansion of the Internet have been witnessed in sexual offences where there is an explosion in the market for online violent sexual pornography crimes, making it easier to create, access, and distribute images of abuse. For example, in February 2014, Lewis Daynes, an eighteen (18) year old unemployed software engineer murdered a fourteen (14) year old boy called Breck Brednar from Redhill, Surrey with whom he groomed online through a gaming site. Police found Brednar in Daynes flat in Grays, Essex and had been stabbed multiple times. Lewis Daynes was sentenced to life imprisonment with a minimum of 25 years (theguardian, 2015). In 2015, attorney David Messerschmitt was murdered in a hotel room in Washington D.C. The police records indicated that David had posted a listing on Craigslist requesting a sexual encounter but was answered by two women who planned to rob him (washingtonblade, 2015). These are just a few instances of what appears to be an explosion of crime and criminality related to the growth of new forms of electronic communication. Since the mid-2000s, the Internet has grown to become a fact of life for people worldwide, especially those living in the Western industrialized world and its relentless expansion keep transforming the spheres of business, work, consumption, leisure, and politics creating new opportunities and challenges associated with living in a 'shrinking' world. We are now said to be in the midst

of a 'new industrial revolution, one that will lead us into a new kind of society, an 'information age'.

Yar (2006) argue that the awareness of, and enthusiasm for, these changes have been tempered by fears that the Internet brings with it new threats and dangers to our well-being and security. 'Cyberspace', the realm of computerized interactions and exchanges, seems to offer a vast range of new opportunities for criminal and deviant activities. A decade or so on from the Internet's first appearance in popular consciousness, the intervening years have been replete with fears about its 'darker', criminal dimensions. Businesses cite threats to economic performance and stability, ranging from vandalism to 'e-fraud' and 'piracy'; governments talk of 'cyberwarfare' and 'cyberterror', especially in the wake of the September 11 attacks; parents fear for their children's online safety, as they are told of perverts and paedophiles stalking the Internet's 'chat rooms' looking for victims; hardly a computer user exists who has not been subjected to attack by 'viruses' and other forms of malicious software; the defenders of democratic rights and freedoms see a threat from the state itself, convinced that the Internet furnishes a tool for surveillance and control of citizens, an electronic web with which 'Big Brother' can watch us all. The development of the Internet and related communication technologies thus appears to present an array of new challenges to individual and collective safety, social order and stability, economic prosperity and political liberty. Community modifications wrought by Internet technologies 'make the future appear not liable to give way and unpredictable', influencing public and political overreaction. Such 'moral panics', powered by the media, lead to an excessive and unjustified belief that particular individuals, groups or events present an urgent threat to society (Critcher, 2013).

2.3 CLASSIFICATION OF VIRTUAL CRIMINAL ACTIVITIES

The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is that it has brought the world closer which has also made it a closely linked place to live in for its users. However, it has also resulted in the creation of a major challenge in the form of Virtual Crimes. There are different Virtual crimes which are taking place in the present world which is dominated by the ICTs. It could be hackers vandalizing your website, viewing confidential information, or stealing trade secrets or intellectual property

with the use of the internet. It can also include 'denial of services' and virus attacks preventing regular traffic from reaching your website.

Virtual crimes also include criminal activities carried out with the use of computers which further perpetuates different crimes, examples includes financial crimes, the sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to the Computer system, theft of information contained in the electronic form, email bombing, physically damaging the computer system (Institute of company secretaries of India, 2016). The number of Virtual Crimes committed is increasing with each passing day, and it is very difficult to find out what a Virtual crime is and what a conventional crime is. However, to deal with this challenge, the most common Virtual crimes can be categorised and discussed under the following heads:

(a) Virtual Crime against Person;
(b) Virtual Crime against Property;
(c) Virtual Crime against Government;
(d) Virtual Crime against Society.

2.4 VIRTUAL CRIMES AGAINST PERSONS

There are certain offences which affect the personality of an individual and include crimes such as Indecent exposure, Pornography (basically child pornography), and the hosting of a website containing these prohibited materials. These obscene conducts may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Attempts have been made in different jurisdictions to combat these criminal activities. Casey (2011:166), for example, posits that in addition to the criminalization of child pornography in the Budapest Cybercrime Convention of the Council of Europe, the Council of Europe's Lanzarote Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (CETS 201) criminalises some other computer-related activities in sexual abuse, including online grooming. Grooming consists of paedophiles establishing a trust relationship with a minor to subsequently meet for sexual abuse. Online grooming, that

is, using the Internet to establish trust, is criminalized by the Lanzarote Convention in Article 23 (Casey, 2011:166).

2.4.1 Ghana Legal Response

In Ghana, the Cybersecurity Act, 2020 (Act 1038) is partly aimed at protecting children and adults from the wrongful and non-consensual exposure of their intimate images in cyberspace Child pornography, revenge pornography, and the non-consensual distribution of private and intimate images have been on the ascendancy in recent times. The Cybersecurity Act responds to these issues by criminalising such conduct with stiff sanctions. Section 136(1) of the Electronic Transaction Act provides that any person "who intentionally does any of the following acts; publishes child pornography through a computer; produces or procures child pornography for its publication through a computer system, or possesses child pornography in a computer system or on a computer or electronic record storage medium commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or both." The Electronic Transaction Act attempts to cast the net wide in addressing abuse of the Internet and the commission of cybercrimes. The provisions of the Act mirror those in several other jurisdictions and introduced into Ghana the institution of cyber inspectors amongst others. The object of the Act, section 1(f), acknowledges that there may be groups of persons in societies that are vulnerable and need protection. To this end, section 1(1) of the Electronic Transactions Act states as one of the objectives the need to "ensure that, concerning the provision of electronic transactions services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account."

2.4.2 United States of America (USA) Legal Response

Communications Decency Act (CDA) of 1996, also called Title V of the Telecommunications Act of 1996, was enacted by the U.S. Congress in response to concerns about easy access to pornography by minors via the Internet, and to combat child pornography. The CDA created a criminal cause of action against those who knowingly transmit "obscene" or "indecent" messages to recipients under the age of 18

years. The Act also prohibited knowingly sending or displaying a "patently offensive" message containing sexual or excretory activities or organs to a minor. The initial stages of the CDA saw a contestation between freedom of expression and the right to protect vulnerable groups, despite the Act making an available defence for those who took reasonably good-faith efforts to exclude children in their distribution or dissemination of such information. Thus *In matter of Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)*, the U.S. Supreme Court struck down those portions of the CDA that banned "indecent" and "Patently offensive" images as being unconstitutionally vague and overboard. However, the rest of the CDA banning the transmission of obscene speech to minors remains in effect.

The United States congress's Child Pornography Prevention Act of 1996 (CPPA) aimed at regulating computer-generated images was also not free of challenges as litigation ensued soon after its passage (Sternberg, 2001:279). As a start, it must be noted that the CPPA prohibits the "production, distribution and possession" of child pornography, with child pornography defined in section 2256 (Title 18) of the Act as "Any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct; (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (D) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct."

For instance, the U.S. Supreme Court rejected the ban on "virtual child pornography." In *Ashcroft v. Free Speech Coal., 535 U.S. 234, 249-50 (2002),* and struck down the CPPA as overboard and violating the First Amendment. Interesting is that the Supreme Court

also questioned the supposed link between computer-generated pornography and the abuse of actual children. It was strange that the U.S Supreme Court did not see the link. Sternberg (2001:2011) argues that what the CPPA did was to enter "into territory protected by the First Amendment by regulating speech solely because it is distasteful," which is something the Supreme Court has always negated in legislation. “If there is a bedrock principle underlying the First Amendment, it is that the government may not prohibit the expression of an idea simply because society finds the idea itself offensive or disagreeable," said the court in *Texas v. Johnson*, 491 U.S. 397,414 (1989).

Be that as it may, after the U.S. Supreme Court invalidated the CPPA, Congress passed the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT Act). The PROTECT Act establishes stronger laws to combat child pornography and exploitation by revising and strengthening the prohibition on computer-generated child pornographic images, prohibiting any obscene materials that depict children, and providing tougher penalties compared to the existing law. The PROTECT Act came against the backdrop of several other laws in 1984, 1986, 1990, 1996, and 1998 that did not wholly succeed in closing loopholes in the law that criminals had found to exploit. It introduced stiff sentences for various offences relating to child sexual abuse material (CSAM). For instance, the minimum prison sentence for a non-family member who abducts a child was raised to 20 years in the PROTECT Act. Furthermore, the PROTECT Act established a 15–30 year sentence for the first offence of using a child to produce CSAM. *In United States v. Williams,553 U.S. 285 (2008),* Supreme Court upheld the convictions of the defendant for one count of pandering child pornography under 18 U.S.C. § 2252A (A)(3)(B) and one count of possessing pornography. Williams received concurrent 60-month prison terms on the two counts.

2.4.3 United Kingdom (UK) Legal Response

The UK (England, Wales, Scotland and Northern Ireland) has a comprehensive legislative and regulatory regime relating to child sexual abuse content (Sexual Offences Act, 2003),. Specific legislation concerning liability for child sexual abuse content was introduced and

has been updated in line with international law and European legislation. A self-regulated notice and takedown system has also been developed for the effective removal of child sexual abuse content under the operation of the national hotline – the IWF. Four main offences exist in the UK relating to the access of sexual images of children, namely: “Possession – possessing sexual images of anyone under the age of 18, whether this is a physical or electronic copy; Distribution – sharing with another person or sending a sexual image of children to another person through different outlets such as chat rooms, email, phone applications, text messaging, USB sticks and file sharing websites; and Making - making an electronic copy of a sexual images” of children.

In terms of section 15a of the Sexual Offences Act (2003), for instance, it is illegal for an adult to intentionally communicate with a child under 16 for a sexual purpose. The offence is sometimes referred to as 'online grooming'. In part to acknowledge the complexity and abuse of the cyber world, the Sexual Offences Act 2003 has been updated with some changes the latest of which came into force on or before 18 October 2022. In England and Wales, the main piece of legislation on child sexual abuse content is the Protection of Children Act 1978 (England and Wales) (the PCA 1978) as amended by several other Acts to respond to new offences and the impact of digital technology. As originally enacted, the Act had as its purpose the prevention of exploitation of children by making indecent photographs of them; and making it possible to punish those that distribute, show and advertise indecent photographs of children. In Scotland, the Civic Government (Scotland) Act 1982 (the CGA 1982) as amended by Section 16 of the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 (the PCPSOA 2005) is the main statute dealing with child sexual abuse content. As for liability of internet service providers for child sexual abuse content, the Electronic Commerce Regulation 2002 is the one that provides certain exemptions for ISPs that do not know about illegal information activity and have no control of it.

Courts in the UK have also made significant rulings regarding the protection of children from exploitation and cyber criminality. This is evident in the matter of *R v. Fellows; R v. Arnold* 1997 the Apeal court convicted Fellows and Arnold of distribution of child

pornography to others on the Internet. In appeal, defence counsel submitted to the court, inter alia, that the data were not "distributed or shown" merely because of its being made available for downloading by other computer users, as the recipient did not view the material held in the archive file, but rather a reproduction of that data which was then held in the recipient's computer after transmission had taken place. The Court of Appeal rejected this argument, holding at p. 558 that the fact that the recipient obtains an exact reproduction of the photograph contained in the archive in digital form does not mean, in our judgment, that the (copy) photographs in the archive are not held in the first appellant's possession with a view to those same photographs being shown to others (*R v. Fellows; R v. Arnold* 1997). The same data are transmitted to the recipient so that he shall see the same visual reproduction as is available to the sender whenever he has access to the archive himself Fellows was sentenced to 3 years in prison and Arnold to 6 months (*R v. Fellows; R v. Arnold* 1997).

In Scotland, indecent child photographs are also deemed illegal. According to Section 52 of the Civic Government (Scotland) Act 1982 (the CGA1982), as amended by Section 16 of the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005 (PCPSOA 2005), it is an offence for a person. Possession of such indecent photographs or pseudo-photographs of a child under 18 years of age also constitutes an offence under Section 52A of the CGA 1982 as amended by the PCPSOA 2005. Similar to the English case law, downloading indecent child sexual abuse images from the internet is deemed as "making" such content in line with Section 52(1) (a) of the CGA 1982. As far as the definition of indecent photographs of children is concerned, for both Section 7 (4) of the PCA 1978 and Section 84 (4) of the CJPOA 1994, photography includes the negatives as well as the positive version, and data stored on a computer disc or by other electronic means which is capable of conversion into a photograph. Concerning the definition of pseudo-photograph, references to a pseudo-photograph include an image, whether made by computer graphics or otherwise, which appears to be a photograph, for the purpose of both Section 7 (4) of the PCA 1978 and Section 84 (4) of the CJPOA 1994. Wei (2011) indicate that, based on the court ruling *of R v. Bowden and R v. Smith with Jayson (*2001 QB 88; 2000 2 WLR 1083), downloading indecent images of children from the internet as well as storing them on the computer or printing them out is another serious

arrestable offence of “making” an indecent image of a child, which will carry a maximum sentence of ten years imprisonment. The UK introduced the Electronic Commerce (EC Directive) Regulations as part of implementing the European Directive on Electronic Commerce into UK law. Among other things, the Regulations provide liability of online service providers for illegal information and activity including those relating to child sexual abuse content. Liability of an ISP under regulations 19 (a) is established only if (i) the ISP has actual knowledge of unlawful activity or information and, where a claim for damages is made, is aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or (ii) upon obtaining such knowledge or awareness, the ISP does not act expeditiously to remove or to disable access to the information. According to Wei (2015:44) as far as ISP liability for child sexual abuse content is concerned, the impact of the 2002 Regulations is that the UK ISPs are encouraged to develop self-regulatory rules and codes of conduct on combating child sexual abuse content over the internet.

2.4.4 Australia Legal Response

Since the advent of the information superhighway and its electronic environment services a two decade ago, Australia legislations concerning cybercrime against persons has been enacted and those pertaining to traditional child pornographic possession has also been enacted amended. The Australian Broadcasting Service Amendment Act 1999 which is which broadly covers issues relating to content regulation and media ownership in Australia has been amended and also the Commonwealth criminal code amendment in 2004 to close the gaps and loopholes that were caused by the advent of the new technology (Alaeldin, 2019:71) Federal and State or Territory laws criminalise child pornography or child abuse-related offences including possession, production, and sale/distribution of child pornography or child abuse materials in Australia and State or Territory are generally responsible for the enactment of child sex-related offences, including child pornography offences, but provisions relating to such offences differ between the various states, in terms of formulation of the offences and the penalties (Wei 2015:44).” Furthermore, Australia legal response to online crimes such as distribution of service attack, denial of service attack, virus and ransomware distribution, identity theft,

virtual fraud, cyber terrorism are mature with many provisions addressing them. At the federal level, the Cybercrime Act 2001 criminalises unauthorise access to computer systems with intent to commit an offense such as identity theft. Wei (2015:43), posit that in Australia, the Federal and State/Territory level have enacted laws that prohibit child pornography and child abuse-related offences. As reported by Wei (2015:43), for eliminating the dissemination of child pornography or child abuse content over the internet, provisions of the Commonwealth's Criminal Code (as amended) create ISPs reporting obligation and that of the Broadcasting Services Act 1992 (as amended) provide a penalty for ISPs "failure to promptly take down child pornography or child abuse content. A mandated notice and takedown procedure has been put in place for the eradication of child pornography or child abuse content over the internet (Wei, 2015:43). In addition, Wei (2015:44) noted that the Commonwealth has also enacted child sex-related offences, including child pornography offences, directed at conducts occurring across jurisdictions, e.g. where the internet is involved. For reasons of brevity, only legislation at the Commonwealth (Federal) level is discussed in this report.

2.4.5 South African Legal Response

One of the advanced countries on the African continent is South Africa. The South African government has enacted Children's Act 38 (2005) to give effect to certain rights of children as contained in the Constitution and set out the principles relating to the care and protection of children. Also, South Africa Child Justice 2008 (Act 75) established a criminal justice system for children, who are in conflict with the law and are accused of committing offences, per the values underpinning the Constitution and the international obligations of the Republic. Child Pornography is also enshrined in the Films and Publications Act, 1996 which defines "child pornography" as any image, real or simulated, however created, depicting a person who is or who is shown as being under the age of 18 years, engaged in sexual conduct or a display of genitals which amounts to sexual exploitation, or participating in, or assisting another person to engage in sexual conduct which amounts to sexual exploitation or degradation of children of any other legislation; or any image, publication, depiction, description or sequence containing a visual presentation, description or representation of pornography or an act of an explicit sexual

nature of a person 18 years or older, which may be disturbing or harmful to, or age-inappropriate, for children, as contemplated in the Films and Publications Act, 1996, or in terms of any other law, to a child, with or without the consent of B, is guilty of the offence of exposing or displaying or causing the exposure or display of child pornography or pornography to a child.

.

2.4.6 Comparative and Legal Analysis

It can be seen from the responses and examination of the child pornography laws of several countries that child sexual abuse content has been a serious concern in Ghana and around the globe. Significantly, efforts have been put in place to eradicate online dissemination of child sexual abuse content. Several legal instruments both national and international provide a baseline legal standard for the protection of children from sexual exploitation. Almost all the countries under study have specific legislation or provisions on child sexual abuse content and ISPs liability concerning online child sexual abuse content, as is the case in Ghana, U.S.A, UK, Australia and South Africa. However, in the countries discussed above, only Ghana does not have the effective tools to investigate specific child sexual abuse content-related crimes, although general provisions on pornographic or obscene materials can still be applied to prosecute child sexual abuse content-related offences.

2.5 VIRTUAL CRIMES AGAINST PROPERTY

As there is exponential growth in international trade between two or more countries where businesses and consumers are increasingly using computers to create, transmit and store information in electronic form instead of traditional paper documents. There are certain offences which affect a person's properties which are as follows: Intellectual Property Crimes: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offense. The common form of intellectual property right violations are software piracy, infringement of copyright,

trademark, patents, designs and service mark violation, and theft of computer source code.

2.5.1 Ghana Legal Response

Ghana, a signatory and a member of many intellectual property organisations, treaties and agreements, including ARIPO, WIPO, TRIPs, Patent Cooperation Treaty, the Paris Convention and the Berne Convention, acts in compliance with standards set by these regimes. Several general principles are important for the effective management of intellectual property ("IP") rights in Ghana. First, it is important to have an overall strategy to protect your IP. Second, IP may be protected differently in Ghana than in the United States. Third, rights must be registered and enforced in Ghana under local laws. The main legislation that protects Ghanaian intellectual property are the Copyright Act, 2005 (Act 690); the Patents Act, 2003 (Act 657); the Trademarks Act, 2004 (Act 664); the Industrial Designs Act, 2003 (Act 660); and the Protection Against Unfair Competition Act, 2000 (Act 589).

The Copyright Act, 2005 (Act 690), passed by the Parliament of Ghana on 17th May, 2005, replaced the previous Copyright law of 1985, P.N.D.C law 110. The act affords protection for eligible artistic and literary work. It also grants holders the right to their creative works and spells out the duration for copyright protection. Significantly, the Act expanded the term of protection for 70 years plus the entire life of the author. the Commercial Crime Unit (CCU) of the Criminal Investigation Department (CID) of the Ghana Police Service is designated to investigate commercial crimes, including IPR infringement.166 However, concerns remain that IP enforcement activity remains weak, and unreasonable delays in infringement proceedings discourage right holders from filing new claims in local courts. The Customs Division of the Ghana Revenue Authority, previously known as Customs Excise and Preventative Service (CEPS), operates under

the Ghana Revenue Authority within the Ministry of Finance. As part of their mandate, the officials of Customs operate at the country's entry posts and are charged with the responsibility of policing Ghana's imports to prevent infringement and illicit products from entering the country.

2.5.2 USA Legal response

Copyright infringement in the form of software piracy is a crime (US Prosecuting Intellectual infringement Crimes, 2006). United State Federal copyright law, which is codified in title 17 of the US Code, protects the "right of authorship" in various kinds of intellectual properties (US Prosecuting Intellectual infringement Crimes, 2006). In order to be protected under US federal copyright law, intellectual property must be "original"; must be "fixed in any "tangible medium of expression"; and must have been registered with the Register of Copyrights (US Prosecuting Intellectual infringement Crimes, 2006). For a work to be "original" it must have "originated" and been created by the author claiming the copyright. Originality does not require novelty but to be original an item cannot simply be a copy of another, pre-existing item (US Prosecuting Intellectual infringement Crimes, 2006). For a work to be "fixed" in a "tangible medium of expression", it must be embodied in a form that is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration (17 US Code§ 101). And while copyright technically attaches when a work is created, the author's registration of the copyright is a prerequisite for a civil action for copyright infringement (17 U.S. Code § 411{a}).

The U.S. Department of Justice takes the position that the registration requirement is only a prerequisite for civil actions; the Department's view is that registration is not a prerequisite for the commencement of a prosecution for criminal copyright infringement (Prosecuting Intellectual infringement Crimes, 2006). Casey (2011:100) assert that Section 506(a) of Title 17 of the U.S. Code makes it a federal crime for someone wilfully to infringe copyright either (i) for purposes of commercial advantage or private financial

gain or (ii) by reproducing or distributing, during any 180 days, one or more copies of one or more copyrighted works having a total retail value in excess of $1000.

Casey (2011:100) further highlight that the basic elements of felony copyright infringement, therefore, are (i) that copyright exited; (ii) that the defendant infringed the copyright by the reproduction or distribution of the copyrighted work; (iii) that the defendant acted wilfully; and (iv) that the defendant reproduced or distributed at least 10 copies of one or more copyrighted works with a total value of more than $2,500 within a 180-day period (18 U.S. Code § 506). In a landmark copyright infringement case involving a peer-to-peer file-sharing service for motion pictures, the U.S. Supreme Court held in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*, 545 U.S. 913 (2005), that "information content providers may be liable for contributory infringement if their system is designed to help people steal music or other material in copyright" the court also held that one who distributes advice with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.

2.5.3 United Kingdom (UK) Legal Response

The United Kingdom (UK) Intellectual property right which concerns the rights of intangible but valuable information or rights covers in particular the United Kingdom Trademark, copyright, and patent law. Copyright law is governed by the United Kingdom Copyright, Designs and Patents Act 1988, as amended from time to time. The modern concept of copyright originated in Great Britain, in the year 1710, with the Statute of Anne. Under the Anne Statute (1710), the copyright term lasted 14 years plus an optional renewal of 14 additional years. The Act came into force on August 1, 1989, save for some minor provisions. Various amendments have been made to the original statute, mostly originating from Copyright law of the European Union and related case law. The Crown

Prosecution Service (CPS) contributes to the enforcement of IP crime in two major ways: firstly, by providing swift, comprehensive and targeted legal advice to police and other investigators; and secondly, by utilising our unparalleled criminal litigation and advocacy experience to prosecute the suspected perpetrators of IP crime in its various forms.

According to the UK Ministry of Justice (2018), 398 people were found guilty of offences under the Trademarks Act in the United Kingdom and 47 under the Copyright, Designs and Patents Act 1988 during 2017, compared with 443 and 47 in the previous year. The number of people cautioned for Trademarks Act and Copyright, Designs and Patents Act offences in 2017 were lower than the previous year. Large-scale and complex cases are handled by the Crown Prosecution Service (CPS) Specialist Fraud Division, based in London and five regional centres. The British Phonographic Industry (BPI) reports a drop of 33% in the number of illegal downloads of bit-torrent and stream rippers. Moreover, total number of downloads fell from 54 million in 2016 to 35 million in 2017 and the Alliance for Intellectual Property outlines collaborative measures taken to mitigate illegal downloading. Also, the Police Intellectual Property Crime Unit (PIPCU) is a department of the City of London Police, the national lead force for fraud. It was established in 2013 with the responsibility to investigate and deter serious and organised intellectual property crime in the United Kingdom. PIPCU is based in the City of London Police's headquarters at Guildhall Yard East. The unit comprises a team of 27 full-time staff including secondments. Part of PIPCU's remit is to protect consumers from harm, focusing on intellectual property crime that has public safety implications. Since its inception, it has investigated intellectual property crime worth more than £700 million concerning counterfeit goods or digital piracy and suspended more than 100,000 websites selling counterfeit goods. These websites have also been linked to identity theft. The Specialist Fraud Division's strong and bespoke relationship with the City of London Police's Police Intellectual Property Crime Unit (PIPCU) has led to a number of successes over the past year in the criminal courts.

In the case of *Queen v Luqman Farooq (2019)*. Luqman Farooq was prosecuted for selling unreleased films online from his bedroom in Halifax. The fraud was far from small

scale, resulting in an estimated loss to the industry of well over £200m. The trial, held on October 2019 at Southwark Crown Court, ended on its second day when Mr Farooq pleaded guilty to conspiracy to defraud and was jailed for 27 months. The case was proved through computer forensics evidence and an important factor in the success of the prosecution was a collaboration between PIPCU, the MPAA, the CPS and the US authorities. Also in the case of the *Queen v Steven Pegram* where the case related to a group calling themselves MiLLENiUM who distributed films online, including "The Expendables 3" through their Foundry website. They were imprisoned for their roles in March 2019, and further details appeared in last year's IP Crime Report. Recently, Steven Pegram sought leave to appeal his sentence of 4.5 years imprisonment on the ground that it was manifestly excessive due to (amongst other things) the delay between his arrest and the case coming to court. His application for leave to appeal was refused, and the Court of Appeal commented that: “The considerations in investigating and prosecuting such sophisticated international fraud dictate that delay in the instigation of the charges is an occupational hazard for these offenders.”

2.5. 4 Australia Legal Response

The Australian Government is responsible for copyright, patents of inventions, designs and trademarks (section 51(xviii), Australian Constitution). Australian Copyright Act 1968 provides civil and criminal sanctions to protect copyright. Copyright may exist at a number of levels, for example, copyright in a song may be held separately for the lyrics, the music, or a particular recording (McRobert, 2001). Exclusive rights may be held concerning the use of the material including moral, transport, rendering, derivative and backup rights. These exclusive rights may, by assignment or licence, be limited in various ways, such as by region or time, or by way of prepaid subscriptions, site-specific licenses, or sponsor-funded licenses (Grabosky, Smith & Dempsey, 2001). The Copyright Act 1968 seeks to balance the interests of owners of intellectual property with the public interest in accessing copyrighted material. It uses a two-stage test of whether a substantial part of a work has been reproduced and whether or not a public interest defence (such as fair dealing) applies. It is recognised that not all infringements can be prosecuted and that law enforcement responses must be appropriate to the circumstances, with adequate means

of supervision and review. In addition, the use of public resources to enforce copyright should be proportionate to the nature of the issue and other policing priorities (Attorney-General's Department, 2003).

It is difficult to estimate the extent and cost of copyright offending (Smith and Urbas, 2003). An industry report by the Business Software Alliance for Australia in 2003 shows a rate of software piracy of 31 per cent, costing an estimated $341 million (Business Software Alliance, 2004). The quantification of loss suffered by copyright holders through internet-based copying is complicated by research that suggests that music downloads have a negligible effect on album sales (Oberholzer with Strumpf, 2007). Breach of copyright is a criminal offence if a person makes, sells, trades or imports an article that infringes copyright in circumstances where they knew or ought to have known of that infringement (Section 132(1) Copyright Act 1968).

It is an offence to simply distribute an infringing item for trade, or to an extent that 'affects prejudicially the owner of the copyright' (s 132(2) Copyright Act 1968). Federal police as well as state and territory police may investigate and commence prosecutions for breaches of federal copyright law. In cases referred to it, the DPP decides the nature and extent of any charges and the manner of presenting the prosecution case (Director of Public Prosecutions Act, 1983). Irrespective of who is involved in an investigation, the Commonwealth Director of Public Prosecutions (DPP) ultimately has the power to take over the prosecution of federal offences. In the 14 years from 1989–90 to 2002–03, the DPP prosecuted 143 copyright cases and 138 trademarks. Formerly distinct non-digital copyrighted formats have converged through digitalization and this has strained the legal framework for copyright protection (Director of Public Prosecutions, 2002).

2.5.5 South African Legal Response

South Africa has enacted copyright laws controlling the use and distribution of artistic and creative work in the Republic of South Africa. It is embodied in the Copyright Act, of 1978

and its various amendment acts and administered by the Companies and Intellectual Property Commission in the Department of Trade and Industry. The copyright Act 1978 draws both from British law and the text of the Berne Convention. The formulation of policy and implementation for patents, trademarks, designs, and copyright is carried out by the Department of Trade and Industry. Copyright registration including property rights, examination of materials, and adjudication is done by the Department of Trade and industry in conjunction with the Companies and Intellectual Property Registration Office (CIPRO). CIPRO is accountable for registering all enterprises, trademarks, designs, and copyrights, as well as conducting hearings in cases of infringement, and arbitration. Copyright Law in South Africa applies to computer programs, literary works, broadcasts, cinematographic films, artistic expressions such as music, photographs, paintings, drawings, sculpting-related works, and architectural works, as well as published editions and sound recordings. With cinematograph films registration is required as such are complex works embedding several other creative works. Currently, South African intellectual property legislation has eighteen pieces of legislation governing intellectual property rights including the Patent Acts 1978, Trademarks Act 1993, Copyright Act 1978, Designs Act 1993, and the Intellectual Property Laws Amendments 1997 (Intellectual Property Act, 1997). While there are laws regarding patents in South Africa, South Africa is a non-examining country (Patents Act, 2002).

2.5.6 Comparative and Legal Analysis

Ghana's Intellectual Property legislation did not make any reference to online intellectual property or any digital goods. Enforcement of copyright infringement is very weak in Ghana unlike the United States, United Kingdom and Australia where Intellectual property infringement sanctions are effective and harsh. The enforcement body such as Ghana Police Service does not have the necessary tool to combat intellectual property offenders. Researchers have shown that copyright protection is very much a technology-related issue with global implications, particularly given the explosion onto the scene of Internet downloads, MP3 Players, Peer-to-Peer Programs, and Web sites enabling, in particular, the availability of music, film, and games. With these new internet applications, there

should be an online expert monitoring Ghana copyright offenders on the internet. Intellectual Property may be protected differently in Ghana than in the United States. Third, rights must be registered and enforced in Ghana under local laws. For example, your U.S. trademark and patent registrations will not protect you in Ghana. There is no such thing as an “international copyright” that will automatically protect an author’s writings throughout the entire world. Protection against unauthorized use in a particular country depends, basically, on the national laws of that country. Granting patent registrations are generally based on a first-to-file or first-to-invent, depending on the country. Similarly, registering trademarks is based on a first-to-file or first-to-use, depending on the country, so you should consider how to obtain patent and trademark protection before introducing your products or services to the Ghana market.

In Australia, the Copyright Act 1968 was updated by the Copyright Amendment (Digital Agenda) Act 2000. However, there has been a cycle of protection followed by the circumvention of each new protective measure. Formerly, distinct non-digital copyrighted formats have been converged through digitalization and this has strained the legal framework for copyright protection. Besides technical issues of proof, the nature of ICT complicates the prosecution of copyright cases. Particular problems are the proof of ownership of copyright and proof that a disputed version is not authorized.

Lastly, most of the Intellectual property rights laws in South Africa are comprehensive and provide extensive coverage for innovators. In recent years, more laws have been drafted and passed to bring intellectual property protection up to international standards. The South African patent system, however, is currently weak and would most likely benefit from more stringent policies.

2.6. VIRTUAL CRIMES AGAINST THE GOVERNMENT

There are certain offences done by a group of persons intending to threaten the international governments by using internet facilities which include cyber terrorism. Cyberterrorism is a major burning issue in domestic as well as a global concern. The common form of these terrorist attacks on the Internet is distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc.

Cyberterrorism activities endanger the sovereignty and integrity of the nation. **"**Today there are many critical sectors whose operations depend vastly on information and computer technology, and therefore it becomes very important to protect these sectors from cyber threat and critically these infrastructures are a complex "system of systems", and the interdependencies amongst these systems are generally not well understood. Disruptions in one infrastructure can propagate into other infrastructures. The operational stability and security of the critical infrastructure are vital for the economic security of the country, and hence its protection has gained paramount importance all over the globe (Clemente, 2015). Zahri, Ahmad, and Yusoff (2014:523) point out that the goal is to protect the county's critical infrastructure by eliminating known vulnerabilities and cyber threats which might oftentimes exasperate to cyber-terrorism. View by Clarke and Knake (2010:260) in trying to know the next threat to national security assert that the acts culminating in the commission of these offences have the severe potential for "a massive cyber-attack on civilian infrastructure that smacks down power grids for weeks, halts trains, grounds aircraft, explodes pipelines, and sets fire to refineries." Networks connectivity to the critical infrastructure continue to grow day by day as new components are being connected to the networks that make up the infrastructure and this allows more efficient operation, but also opens those components to serious network attacks.

The consequential rise in these attacks, together with the vulnerabilities of these infrastructure networks have led many countries' leaders and their governments to recognize the enormity of the issue, resulting in a push for increasing mandated cybersecurity covering both government and private networks; and enacting specific legislation to protect them. In 2005, the European Council adopted the European Program for Critical Infrastructure Protection (EPCIP) to focus on strengthening information systems, and enhancing preparedness for cyber-attacks on the networks and computer systems that form part of the critical national infrastructure (European Programme for Critical Infrastructure Protection, 2005).

2.6.1 Ghana Legal Response

In Ghana, the landmark Cybersecurity Act 2020 protects the critical information infrastructure of the country, regulates cybersecurity activities, and develops Ghana's cybersecurity ecosystem. The Ghana Cybersecurity Act (2020) Section 3b provides that, the major objectives for the enactment of the Act is to prevent, manage and respond to cybersecurity threats and cybersecurity incidents and Section 4b of the Act is to promote the security of computers and computer systems in the country. The components of this infrastructure include computers, computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data, content data and/or traffic data so vital to the country that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

Due to the evolving and dynamic nature of virtual crime or cybercrime section 4g of the Act provides measures that will be taken in response to cybersecurity incidents that occur within and outside the country which may threaten (i) national security; (ii) the defence of the country; (iii) the economy of the country; (iv) international relations between the State and other countries; (v) health of the public; (vi) the safety of life and property; and (vii) any other sector of the country likely to be affected by a cybersecurity incident. And section 4(h) will identify and designate critical information infrastructure and advise the Minister of Communication on the regulation of owners of critical information infrastructure to protect the critical information infrastructure of the country, in accordance with international best practice.

2.6.2 U.S. A Legal Response

The USA on the other hand has primary federal statutes used to prosecute cybercrime. The United States focuses on the Computer Fraud and Abuse Act, as the state statutes criminalizing identity theft, child pornography, copyright and trademark. The Computer Fraud and Abuse Act of (1986) which was codified as § 1030 of Title 18 is the U.S. Code adopted by congress in 1986, but it has since been amended on several occasions. Section1030(a) of the Act criminalized gaining unauthorized access to a computer,

disseminating malware, launching denial of service attacks, trafficking in passwords, and using computers to commit fraud or extortion. Increased instances of cyberspace abuses in the 1980s spurred Congress to significantly revise the CFAA in 1986. Since 1986, Congress has amended the CFAA nine times to keep pace with technological advances and counter the evolving sophistication of computer crimes (Exec. office for U.S. attorneys, prosecuting computer crimes 2007). Most significantly, following the September 11th attacks and enactment of the 2001 USA PATRIOT Act, Congress explicitly conferred extraterritorial application on the CFAA. The USA PATRIOT Act expanded the CFAA's definition of "protected computers" to include computers that affect "interstate or foreign commerce or communication," regardless of whether they are located outside of the United States (Doyle, 2005:97). For example, in *United States v. Trotter*, the Eighth Circuit held that the defendant's damage to his former employer's computer network violated the CFAA. Since the computer network was connected to the Internet, it was used for "interstate communication" and therefore constituted a "protected computer" under the statute. 478 F.3d 918 (8th Cir.2007). More recently, in *Freedom Banc Mortgage Services v. O'Harra,* the district court held that a computer fulfilled the definition of a "protected" computer under the CFAA by virtue of its merely being connected to the Internet. 2012 U.S. Dist. LEXIS 125734 (S.D. Ohio 2012). Also in *United State v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001)* holding that a Russian defendant's hacking into a Connecticut corporation's computer connected to the Internet constituted unauthorized access of a protected computer within the meaning of the CFAA.

Since courts have expansively interpreted "protected computers" to include any computer connected to the Internet, the CFAA prohibits knowingly or recklessly damaging the vast majority of computers within the U.S.76 Furthermore, the provisions of "exceeds authorized access" can be interpreted to preclude cyberterrorist botnet attacks. Since Congress conferred extraterritorial reach on the CFAA and the other aforementioned statutes, applying such statutes to cyberterrorists abroad would accord with the first canon of statutory construction. To comply with the second canon, the Charming Betsy doctrine, the United States must prosecute cyberterrorists abroad predicated on one of the five accepted bases of prescriptive jurisdiction under international law. Although Congress could have chosen to negate the Charming Betsy doctrine, the legislative

history of these statutes and their subsequent amendments do not indicate any intent to contravene international law.

2.6.3 United Kingdom (UK) Legal Response

The Computer Misuse Act 1990 is an Act of the parliament of the United Kingdom, introduced partly in response to the decision in *R v Gold with Schifreen* (1988) 1 AC 1063 where the defendant was acquitted because there were no laws to prevent unlawful access to a computer. This "led to the enactment of the Computer Misuse Act 1990. However, this act was soon found to be ineffective in addressing cybercrime (McKenna 2004). The UK's ratification of the Council of Europe's Convention on Cybercrime also led to calls to amend the Computer Misuse Act 1990 (CMA). The CMA was consequently amended on 1 October 2008 to clarify the meaning of "unauthorised access" to a computer (Fafinski 2008:53). The inclusion of a new provision also makes it an offence to make, adapt, supply or offer to supply any item of hardware, software or data for use in the commission of an offence under the Act (Fafinski 2008:48). The United Kingdom Home Office had recently sponsored the Serious Crime Bill in June 2014 as part of the Queen's Speech opening the 2014-15 session of Parliament (United Kingdom Home Office, 2014). This Bill received royal assent on 3rd March 2015 and is now known as the Serious Crime Act 2015. Part two of the Act implements the EU Directive on Attacks against Information Systems and also amends the Computer Misuse Act 1990 in relation to hacking offences, by creating a new offence of unauthorised acts of causing serious damage. The Serious Crime Act also creates a new offence of impairing a computer to cause damage, and further prescribes a severe punishment of up to 14 years' custodial sentence for cybercrime offences that result in damage to the economy or environment.

2.6.4 Australia Legal Response

Research has shown that the Australian Government’s vision is to create a more secure online world for Australians, their businesses and the essential services upon which we all depend. Australians are increasingly reliant on the internet and the internet-connected devices we use daily (Australian Government, 2020). Australia has established some key

cybersecurity centres such as the Australian Cyber Security Centre (ACSC) to engage the state and territory governments and industry increasing cyber skills and education (Australian Cyber Security Centre, 2017). The Australian Cyber Security Centre (ACSC) leads the Australian Government's operational efforts to improve cyber security and help make Australia the most secure place to connect online. The ACSC is part of the Australian Signals Directorate (ASD) and is a hub for private and public sector collaboration and information-sharing on cyber security to prevent and combat threats and minimise harm to Australians. ACSC provides advice and assistance across the whole economy, including critical infrastructure and systems of national interest, federal, state and local governments, small and medium businesses, academia, not-for-profit organisations and the Australian community.

The Australian Cyber Security Centre (ACSC) with the help of the Australian Federal Police's enforce commonwealth criminal, and contribute to combating complex, transnational, serious and organised crime impacting Australian national security and protecting Commonwealth interests from criminal activity in Australia and Overseas (Australia Federal Police, 2018). Australia's laws against terrorism are in Part 5.3 of the *Criminal Code Act 1995*- external site (Criminal Code). The Counter-Terrorism Legislation Amendment Act 2019 prohibits terrorism in Australia. The Model Criminal Code and Cybercrime Act 2001 also advocate computer-related crimes. The inadequacy of the existing criminal laws to address computer misuse and computer offences has led to calls for distinct statutory laws for computer offences to keep up with modern technology.

Thus Australian citizens who commit computer offences in countries that have no real or important links to their home jurisdiction can now be prosecuted in terms of the Commonwealth. To illustrate this*, the case of Director of Public Prosecution v Sutcliffe,* (2001 VSC 43 Victoria, Australia), suggested that laws allowing the police to rapidly secure evidence stored on computers and to obtain real-time access to network traffic may be needed for Australia to join a global treaty aimed at fighting fraud and electronic crime. an Australian citizen, Brian Sutcliffe, was accused of stalking a Canadian actress who lived in Toronto. The charges were based on Sutcliffe's having telephoned the victim

and written to her repeatedly over several years (Director of Public Prosecution v Sutcliffe, 2001). The Australian prosecutor charged Sutcliffe with stalking but the magistrate dismissed the charges. The magistrate found that she lacked jurisdiction to adjudicate the matter because the crime of stalking occurred in Canada, where the victim was located. However, the Supreme Court of Victoria reversed the decision (Director of Public Prosecution v Sutcliffe, 2001). The Court found that Sutcliffe was a resident of Australia and had committed all of the ingredients of the crime "save for the harmful effect" in an Australian court to exercise jurisdiction over the proceedings (Director of Public Prosecution v Sutcliffe, 2001).

2.6.5 South Africa Legal Response

South Africa has introduced a number of legislative measures to address the growing threat to critical information and communication technology infrastructure by cyber-terrorists. Currently, the Cybercrimes and Cybersecurity Act (Act 2020) was signed into law by South African President Cyril Ramaphosa in early June 2021, bringing the country's cybersecurity legislation in line with global standards (Cybercrimes Act, 2020). The Act compels electronic communications service providers and financial institutions to act when they become aware that their computer systems have been involved in a cybersecurity breach, as defined by Act. Chapter 8 Section 54(part 1) of the Act states category that any electronic communications service provider or financial institution that is aware or becomes aware that its electronic communications service or electronic communications network is involved in the commission of any category or class of offences provided for in Part I of Chapter 2 and which is determined in terms of subsection (2), must— (a) without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and (b) preserve any information which may be of assistance to the South African Police Service in investigating the offence (Cybercrimes Act, 2020).

Section 14 of the cybercrime and Cybersecurity Act states that any person who discloses, by means of an electronic communications service, a data message to a person, group of persons or the general public with the intention to incite— (a) the causing of any damage to property belonging to; or (b) violence against, a person or a group of persons, is guilty of an offence. The cybercrime and Cybersecurity Act intends to further regulate the powers to investigate cybercrime and also criminalize harmful data messages that invite or threaten violence or damage to property, as well as those that contain intimate images (Cybercrimes and Cybersecurity Act 2020). Data is broadly defined in the Act as "electronic representations of information in any form. And also criminalizes cyber fraud, extortion, forgery and theft of incorporeal property. The unlawful accessing of a computer system, data storage medium or personal data is an offence prohibited and offence leading to hefty fines and lengthy prison sentences of up to 15 years. In South Africa, data security is also governed by the Protection of Personal Information Act (POPIA). This legislation, among other things, promotes the protection of personal information processed by public and private bodies, outlines the rights of data subjects, regulates the cross-border flow of personal information, introduces mandatory obligations to report and notify data breach incidents, and imposes statutory penalties for violations of the law." On top of the above legislations, South Africa has the Terrorism Act (1967), Organised Crime Act 38 (1999) Financial Intelligence Centre Act 38 (2001) the Electronic Communications and Transactions Act 25 (2002).

2.6.6 Comparative and Legal Analysis

Comparatively, laws in these four countries under study did not make any specific reference to cyberwar or cyberterrorism attacks, but rather highlight or opine at setting out a broad framework addressing communication interruption and destruction of data. The United States, United Kingdom and Australia impose harsh sanctions for the offender of crimes committed on government or state infrastructures, unlike Ghana which imposes a sanction that is not too harsh. The Ghanaian legislation on infrastructure attacks or cyber terrorism is so broad and it includes both physical attacks such as bomb attacks. There is no definition for cyber war, or cyber terrorism in the Ghanaian cybersecurity Act (2020). The National Information Infrastructure Protection Act of 1996 (hereinafter, the

NIIPA or 'the 1996 Act') protects individuals against various crimes involving protected computers (Bazelon, Choi,& Conaty 2006:260). Both the US Secret Service and the FBI have jurisdiction over offences committed under the NIIPA, the latter through the USA Patriot Act (1030 (d) of the NIIPA). The Electronic Communications Privacy Act of 1986 (hereinafter the ECPA) is also aimed at non-traditional crimes such as hacking. It prohibits any obtaining, altering or preventing unauthorised access to electronic storage

Federal offences include cyber fraud, identity theft, spamming, cyber stalking, cyber fraud, making intentional false representations online, identity theft, the use of password sniffers, the decimation and creation of worms as well as the writing of viruses and Trojan horses, website defacements and web-spoofing (Snail & Madziwa 2008:30). Many states such as Arkansas and California have enacted anti-spam laws to regulate the use of Internet communications that send unsolicited advertisements for promoting real property, goods, or services for sale or lease. Statutes have also been enacted in some states such as Arkansas and Georgia to provide civil compensatory damages to encourage the victims of computer crimes to come forward. (Bazelon Choi & Conaty, 2006:304).

Considering the Australian legislation on cybersecurity that enforce critical infrastructure, Some academic writers advocate the participation of private actors and stakeholders such as credit card companies and corporations in the fight against cybercrime, because these stakeholders have a vested interest (Bronitt & Gani, 313-317) Janine Wilson also calls for effective partnerships with the private sector and international entities to effectively manage and combat cybercrime (Wilson 2006:694). The involvement of the private sector will help to improve the ability of law enforcement (the police) to effectively perform its role of combating cybercrime, and will also assist the private sector to address cyber threats. This will also help to minimise financial damage. In Australia, the role of the financial services industry in targeting cybercrime developed because of its being targeted by cybercriminals, and in this regard, the Australian Bankers Association has undertaken many projects addressing the problem of rising levels of cybercrime (Wilson, 2006:694). The UK experience demonstrates that the UK is trying its best to keep cyber criminals at bay: the increase in the penalty for unauthorised access to a computer (from

six months to two years) and the criminalisation of the denial of service attacks illustrate a tougher stance on cybercrime. Innovative proposals aimed at child sex offenders have been introduced by the Home Office. The advent of the National Hi-Tech Crime Unit has also been lauded This initiative, which brings the police, the private sector and academics together to combat cybercrime, ensures the participation of all of the key parties in the fight against cybercrime (Wilson 2006:694) .

2.7 MOTIVES AND CAUSES OF VIRTUAL CRIMINALS

To get an understanding of what the virtual criminals are doing with the destructions and stolen data, and how they are monetizing the data, we need to understand who they are and what motivates them. Virtual Criminals or attackers on the internet can be categorized by their set of goals, motivations, and capabilities. Robinson *et al* (2013:106) highlight the four groups of note are cyberterrorists, hacktivists, state-sponsored actors, and cyber criminals. Ablon (2018:2) reveals that cyber criminals unite two significant modern concerns: attacks via technology in cyberspace and traditional crime. Hoffman,(2012:149) asserts that while there is no single or globally accepted definition of cybercrime, in theory, it consists of a politically motivated criminal group or non-state actor using cyber techniques to intimidate, coerce, or influence an audience; force a political change, or cause fear or physical harm. Ablon (2018:2) points out that there have been no publicly reported cases of terrorists using the internet to carry out cyberattacks and what has been attributed to cyberterrorism is more akin to hacktivism. Many terrorists, or nonstate actors, do employ cyber to further their goals (Ablon 2018:2). This is supported by Mueller (2012) that they use the internet in many ways: for information gathering, e.g., learn how to build a bomb; to recruit, meet, and connect with like-minded individuals; and to spread propaganda. But just "being" in cyberspace does not make a terrorist a cyberterrorist. Cyberspace must be used somehow to commit a terrorist act Conway (2007:73).

Passeri (2012) states that hacktivists are typically motivated by a cause—political, economic, or social: from embarrassing celebrities to highlighting human rights, to waking up a corporation to its vulnerabilities, to going after groups whose ideologies they do not agree with. In his paper, Ablon (2018:3) further adds that hacktivists may steal and

disseminate sensitive, proprietary, or, sometimes, classified data in the name of free speech. Other times, they aim to deny access to a particular service or website by conducting a distributed denial-of-service (DDoS) attack, essentially denying legitimate access by flooding a website with more traffic than it can handle, causing the site to crash. According to Ablon (2018:40), state-sponsored cybercriminals receive direction, funding, or technical assistance from a nation-state to advance that nation's particular interests. State-sponsored actors have stolen and infiltrated intellectual property, sensitive personally identifying information (PII), and money to fund or further espionage and exploitation causes. In rare cases, these data appear for sale on underground black markets. Instead, these data are usually kept by the actors for their purposes. Although, Ablon (2018:47) highlights that the data taken from data breaches might not always appear on underground markets, what can appear are the tools and guides for how to take advantage of the vulnerabilities that allowed access to the vulnerable systems in the first place. As an example, a researcher published the flaw that was used to penetrate Equifax, and within 24 hours the information was published to hacking websites and included in hacking toolkits.

State-sponsored cybercriminals have conducted cyberattacks to deny, degrade, disrupt, or destroy computing systems and to send a political message. An example of this is the 2014 attack on Sony Pictures Entertainment, where North Korea wanted to advance its political agenda and, in part, to stop the release of the movie The Interview (Federal Bureau Investigation, 2014). Cybercriminals are also motivated by financial gains by intruding into personal, financial or health data to sell or monetize them in underground black within days. The underground black markets are dispersed, diverse, and segmented, rapidly growing, constantly changing, and innovating to keep pace with consumer trends and prevent law enforcement and security vendors from understanding them. The underground black is dedicated to one product and or specialized service. Cybercriminals operate behind anonymous and peer-to-peer networks and use encryption technologies and digital currencies such as Bitcoin to hide their communications and transactions (Ablon, 2018:47). Case example is the federal criminal charge for Matthew Gatrel, 32, of St. Charles, Illinois, for operating Subscription-Based Computer Attack websites that allowed paying users to launch powerful distributed denial

of service, or DDoS, attacks that flood targeted computers with information and prevent them from being able to access the internet (United States Attorney's Office, Central District of California Los Angeles 2021). Matthew Gatrel, 32, of St. Charles, Illinois, was found guilty of three felonies: one count of conspiracy to commit unauthorized impairment of a protected computer, one count of conspiracy to commit wire fraud, and one count of unauthorized impairment of a protected computer. According to evidence presented at his nine-day trial, Gatrel owned and operated two DDoS facilitation websites: DownThem.org and AmpNode.com. according to the United States Attorney's Office, Central District of California Los Angeles (2021) DownThem sold subscriptions allowing customers to launch DDoS attacks while AmpNode provided "bulletproof" server hosting to customers with an emphasis on "spoofing" servers that could be pre-configured with DDoS attack scripts and lists of vulnerable "attack amplifiers" used to launch simultaneous cyberattacks on victims.

United States Attorney's Office of Central District of California, Los Angeles (2021) also posits that records from the DownThem service revealed more than 2,000 registered users and more than 200,000 launched attacks, including attacks on homes, schools, universities, municipal and local government websites, and financial institutions worldwide. Often called a "booting" service, DownThem itself relied upon powerful servers associated with Gatrel's AmpNode bulletproof hosting service United States Attorney's Office (Central District of California Los Angeles, 2021). Many AmpNode customers were themselves operating for-profit DDoS services. United States District Judge John A. Kronstadt scheduled a January 27, 2022 sentencing hearing, at which time Gatrel faced a statutory maximum sentence of 35 years in federal prison. Co-defendant Juan Martinez, 28, of Pasadena, pleaded guilty on August 26 to one count of unauthorized impairment of a protected computer. Martinez was one of Gatrel's customers and became a co-administrator of the site in 2018. Martinez will face a statutory maximum sentence of 10 years in federal prison at his sentencing hearing, which is scheduled for December 2 (United States Attorney's Office, Central District of California Los Angeles 2021). Often there is not enough digital evidence left behind to identify the attackers or their country of origin but there are cases where various information and communication technology security firms and incident response experts, and threat, analysis groups involved in the

aftermath of a breach have found similarities in the malware used in various attacks and the above case is a typical example. According to Ablon (2018:47), there are distinctions and differences in motivation between each of the cybercriminals, there is some degree of fluidity between the groups. In many cases, the same tools and techniques are used by different groups, sometimes because those are the only tools available, and other times because that helps with plausible deniability and shifting the blame to a different group. In some countries, state-sponsored actors may work with “citizen hackers” or their country’s cybercriminal elements to carry out an attack (Ablon 2018:47).

2.8 CHAPTER SUMMARY

The tremendous growth in the field of information and communication technology coupled with an increased frequency of use of the internet for different activities has also given rise to several mischievous activities taking place in the form of virtual crime or cybercrime. The exponential expansion of computer technology and the internet has spawned a variety of new criminal behaviours and has provided criminals with a new environment within which to operate. Since the mid-1990s, the Internet has grown to become a fact of life for people worldwide, especially those living in the Western industrialized world. Its relentless expansion, it is claimed, is in the process of transforming the spheres of business, work, consumption, leisure, and politics (Castells, 2002:102). As a result of that, efficient legal response to virtual crime offences is a prerequisite to success in searching and seizing computers and obtaining digital or electronic eviden

CHAPTER THREE

COMPUTER FORENSICS AND VIRTUAL DETECTIVE WORK

3.1 INTRODUCTION

Forensic Science has become popular in recent times, the popularity of Television shows involving forensics has propelled forensics into the forefront of the public view on solving various types of crimes. The term forensic is defined basically as "science used for the purpose of law" (White, 2016:56). Forensic science as it is recognised today traces its beginning back thousands of years and was driven by the need to investigate suspicious deaths. The origins of forensics date back to the 6th century in Chinese history, however, it was not before the 18th century that the true types of forensic evidence as we know it today began to emerge. Forensic science has its roots in law and is sometimes referred to as forensics which itself means the application of science to law. Information and communications technologies (ICT) are fundamental to modern society and open the door to increased productivity, faster communication capabilities, and immeasurable convenience. However, the era of ICT-enhanced globalisation has also been accompanied by an increase in the sophistication and volume of malicious cyber activities. Computers and networks have become so ubiquitous in our society, such an integral part of our daily lives that any investigation or a legal dispute will likely involve some form of digital evidence electronic evidence and information gathering have become central issues in an increasing number of conflicts and crimes. Currently, there is a laborious paradigm shift in computer investigation and it requires significant expertise on the part of the investigators. Crimes like child exploitation, fraud, drug trafficking, terrorism, and homicide usually involve computers to some degree (Eoghan, 2012:145). Within the past few years, a new class of crime committed with the use of computers and their devices has become more prevalent. These new increases in criminal activity pose or deter business organisations, government and law enforcement. Hence the need to shift from document-based evidence to digital or electronic evidence has necessitated a rapid reformation of standards and procedures (Eoghan, 2012:222). Increasingly, criminals are using technology to facilitate their offences and avoid apprehension, creating new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals. Organized criminals around the globe are using technology to maintain records, communicate, and commit crimes. Electronic discovery has become so common in civil disputes that countries are updating their legal guidelines to address digital evidence. Vacca (2013:51) contend that Computer forensics,

also referred to as computer forensic analysis, electronic discovery, electronic evidence discovery, digital discovery, data recovery, data discovery, computer analysis, and computer examination, is the process of methodically examining computer media (hard disks, diskettes, tapes, etc.) for evidence.

A thorough analysis by a skilled examiner can result in the reconstruction of the activities of a computer user. In other words, computer forensics is the collection, preservation, analysis, and presentation of computer-related evidence. It has become a necessity for an organisation to either employ the services of a computer forensic agency or hire a computer forensic expert to protect the organization from computer incidents or solve cases involving the use of computers and related technologies. Xiaoyu, Nhien, and Mark (2017:573) claim that the field of digital forensics has become commonplace due to the increasing prevalence of technology since the late 20th century, and the inevitable relevance of this technology in the conducting of criminal activity. Xiaoyu *et al* (2017:573) write that in traditional forensics, the evidence is generally something tangible that could identify the criminal, such as hair, blood or fingerprints. In contrast, digital forensics deals with files and data in digital form extracted from digital devices. Digital forensics is a widely-used term, referring to the identification, acquisition and analysis of digital evidence originating from much more than just computers, such as smartphones, tablets, Internet of Things Devices, or data stored in the cloud. Computer forensics, a relatively new sub-discipline of forensic science when compared to other common forensic science disciplines, is the process of gathering evidence of some type of an incident or crime that has involved computer systems and their associated networks (Martini & Choo 2012; Quick, Martini & Choo 2014).

3.2 COMPUTER FORENSICS AND SUB-DISCIPLINE

Larry and Lars (2012:18) posit that computer forensics is the oldest of the sub-disciplines but makes up digital forensics. Computers are often the main source of digital evidence in a case, and with good reasons (Larry & Lars, 2012:18). Computers can contain a massive amount of useful information in a case in and of themselves and can contain

useful information about other devices like USB thumb drives, cell phones, digital cameras, and portable hard drives because almost all devices at one point or another circle back around to a computer (Larry & Lars, 2012:18). For example, to create a backup of the information on your cell phone, it has to be connected to the computer. The same is true if you want to remove the pictures from a digital camera or USB thumb drive. Computer forensics is primarily the examination of evidence found on a computer hard drive, such as user accounts, log files, time stamps, images, e-mails, and in some instances the examination of data on other hardware components within the computer, like the memory. Computer forensic sub-disciplines can be categorised as:

3.2.1 Cell phone forensic

Mobile phones are a special case of embedded systems. They are small, typically pocket-seized, and they have some constraints with regard to screen size, power usage, input methods, and so on. Ayers, Brothers and Jansen (2014:85) refer to the definition by the National Institute for Science and Technology (NIST) of mobile forensics as “the science of recovering digital evidence from a cellular device under forensically sound conditions using accepted methods.” In support of this statement by NIST,. Larry and Lars (2012:18) highlight to include the examination of cell phones, as well as the records created by cell phone service providers like cell phone billing information and call detail records (CDRs). Call detail records contain information about the numbers that were called from a particular phone, the duration of the call, the date and time of the call, and the cell site information for cell phones (Larry & Lars, 2012:18). Cell site information can provide information as to the general location of a person and their movement based on their cell phone activity. However, using phone records to establish the where about of a person by their cell phone activity is highly subject to the proper analysis of the cell site location information, the call detail records, and correct historical analysis of the cell site data. The examination of cell phones has become as common as the examination of someone you know who does not own a cell phone. Cell phones contain a wealth of information, and examining them can recover data of evidentiary value such as contacts on a phone, text messages, images, video, audio recordings, and e-mail. Mobile forensic toolkits are

available in the market including Oxygen forensics, Cellebrite's Universal Forensic Extraction Device (UFED), and XRY Forensic Examiner's Kit (Jones & Winster, 2017:8). These tools help to extract certain informative data. Choo and Dehghantanha (2016) outline that the basic information obtained from mobile phones, despite the device differences are:

(a) Phone Storage Data,
(b) Messages: SMS, MMS, E-Mails,
(c) Social Media Data,
(d) Call Records: Missed/Outgoing/Incoming Calls,
(e) Multimedia Data: Photos, Videos and Audio files,
(f) Communication Network Data

As Cahyani, Rahman, Glisson, and Choo (2017:240) posit, existing mobile forensic research can be classified into:

(a) examining the capabilities of acquisition methods,
(b) undertaking detailed forensic procedures, and
(c) conducting in-depth forensic analysis of mobile apps or mobile operating systems.
(a) As an example, Sathe and Dongre (2018:280) presented their experimentation on the data extracted from Samsung Galaxy Grand Duos GT I9082 mobile device by using AFLogical OSE, Andriller and Wondershare Dr Fone for Android tool. The results shown below demonstrate the difference in the data extraction from each tool:
(b) AFLogical OSE: messages, call logs;
(c) Andriller Tool: messages, call logs, web browser, wifi password, accounts;
(d) Wondershare Dr. Fone for Android: messages, call logs, contacts, images, audio, video, documents, WhatsApp message and attachments. (both deleted and undeleted data)

3.2.2 Geographical positioning systems (GPS) forensics

Faqir (2013:433) posits that Global Positioning Devices (GPS) technology is a satellite-based technique that reveals the site of a given location. The GPS is a new advanced high technology designed for a satellite navigation system used for multi-purposes in several fields of life. Bellis (2013) contends that in the beginning, it was utilized only for marital purposes in the United States and then later became available for civil use by states, companies and even individuals. All the enabled devices of GPS are on sale in global markets for personal, organisational and official use by states. GPS records are also valuable as evidence and can be used to see the movement of a person or vehicle. By examining the data available in GPS units, it is possible to estimate how best someone was driving, if they made any stops and for how long. If a person is suspected of a crime, GPS records can help determine if that person went to the location where the incident happened, whether they were ever near it in the vehicle, or if the timeframe even allows for the possibility of that person being a suspect. For instance, assume that a suspected person is accused of committing a murder at one location, and then dumping the body at another within a one–hour timeframe, if it takes an hour and a half to drive the distance from the scene of the incident to the location of the body.

The usage of such technology has different aspects in the present industry; it is used in cars and phone mobiles which help in determining directions and locations. In the last decade, the industry of GPS occupied the attention of the criminal justice system and law enforcement agencies as it became one of the effective means of criminal investigation. An electronic tracking device (also called a transponder) is a one-way radio communication device that emits a signal on a specific radio frequency. This signal can be received by special tracking equipment and allows the user to track the geographical location of the transponder. Faqir (2013:437) asserts that electronic tracking can be distinguished from electronic surveillance equipment in that the location of the subject is the primary goal of tracking. Surveillance involves seeing or hearing the subject. Prior to electronics, tracking meant following the trail of evidence left behind by the subject: his or her scent, fingerprints, and footprints (Gale, 2006). As prices have dropped for GPS, and the technology has gotten better, they have become much more common. Today, for example, many vehicles have a GPS tracking device in them, such as rental cars, that the driver probably does not even know about (Larry & Lars 2012:18). GPS forensics

includes the examination of GPS units as well as GPS records. The examination of GPS units can yield information such as recently visited locations, favourite locations, and locations navigated by address or street intersection. It is also possible to recover deleted information from many GPS units.

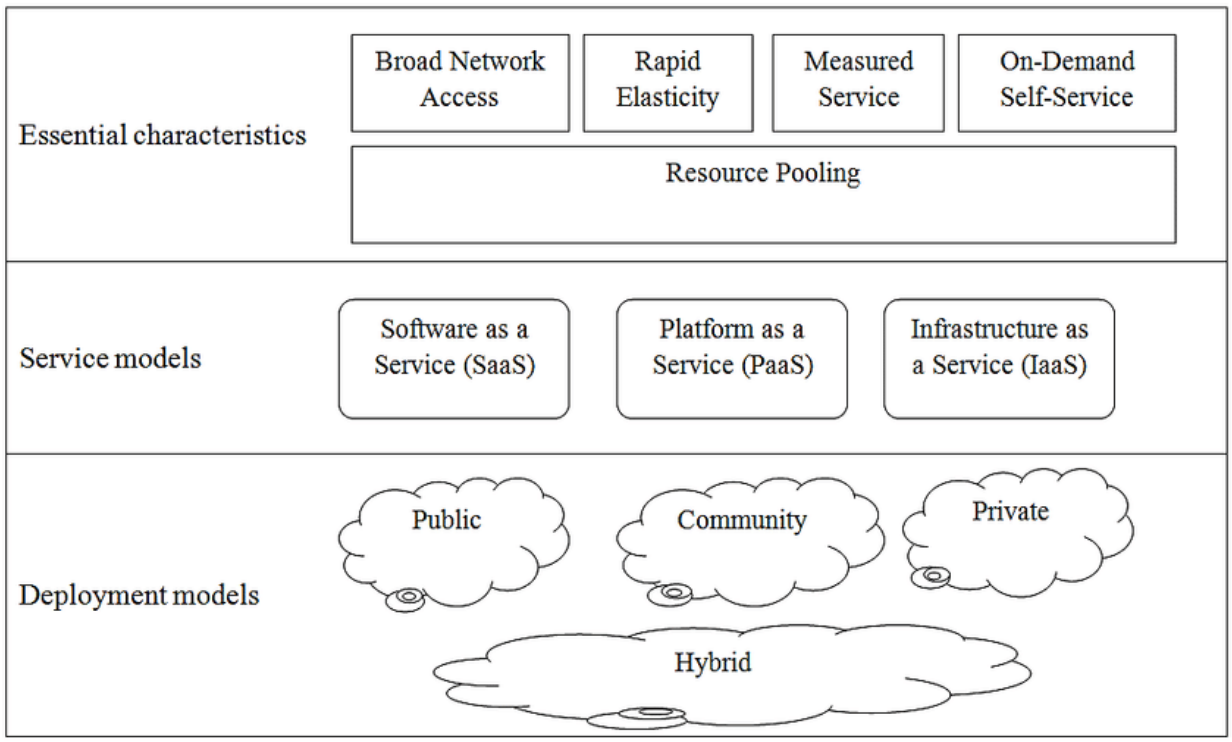
3.2.3 Cloud forensics

Orwoh *et al* (2013:608) contend that Cloud computing has gained popularity because it offers various benefits including convenience, large capacity, scalability, and on-demand accessibility. Cloud computing is a style of computer where scalable and elastic IT-related capabilities are provided 'as a service to multiple external customers using Internet technologies (Gartner, 2011). Cloud Security Alliance (2011) defines cloud computing as “an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimised and efficient computing.” However, attacks being discovered and exploited in various cloud-related crimes have led to a need for digital forensics in the cloud environment. Precise definitions and understanding of terms related to new technologies can be various at times (Du, 2020:11). To better understand cloud forensics, such as its definition, scope, challenges, opportunities as well as missing capabilities, a survey among digital forensic experts and practitioners was conducted by (Ruan ,Carthy, Kechadi & Baggili 2013: 34). According to the results, the respondents believe that cloud forensics is not Internet forensics or classical computer forensics, nor a brand-new area (Du, 2020:12). It is rather a mixture of traditional forensic techniques and their applications in a cloud computing environment (Du, 2020:12). Pichan, Lazarescu, and Soh (2015:38) grouped the investigation into three areas, (i) Client forensics (ii) Cloud forensics, and (iii) Network forensics. According to Du (2020:12), cloud-based file synchronisation services have become very popular, which offer a remote backup of data paired with the automation of data across multiple devices. Du, Le-Khac, and Scanlon (2014:85) in their research contribution in 2014, state that a

methodology was outlined enabling the recovery of remote digital evidence from a decentralised file synchronisation network, as a result, extends the digital evidence acquisition window. Teing, Dehghantanha, and Choo, (2017:30) presented the types and locations of CloudMe residual artefacts on desktop and mobile client devices running Windows 8.1, Ubuntu 14.04.1 LTS, Mac OS X Mavericks 10.9.5, iOS 7.1.2, and Android KitKat 4.4.4.

The cloud computing definition by the NIST identifies five crucial characteristics which are described below as shown in Figure 3.1 (The NIST Cloud Computing Reference Architecture SP 500-292)

(i) On-demand self-service: A user can automatically provision cloud capabilities without needing human interaction with every service request.
(ii) Broad network access: It means can provide cloud capabilities which can be accessed over the network using standard devices.
(iii) Resource pooling: The cloud resources are pooled to serve numerous users using a multi-tenant paradigm.
(iv) Rapid elasticity: The cloud capabilities can be provisioned and released elastically.
(v) Measured service: Cloud resource use can be optimised and controlled automatically by leveraging a metering ability which is suitable to the service type.



- Figure 3.1: Cloud Computing Framework (Source: Katarzyna et al (2012).

3.2.3.1 Deployment Models

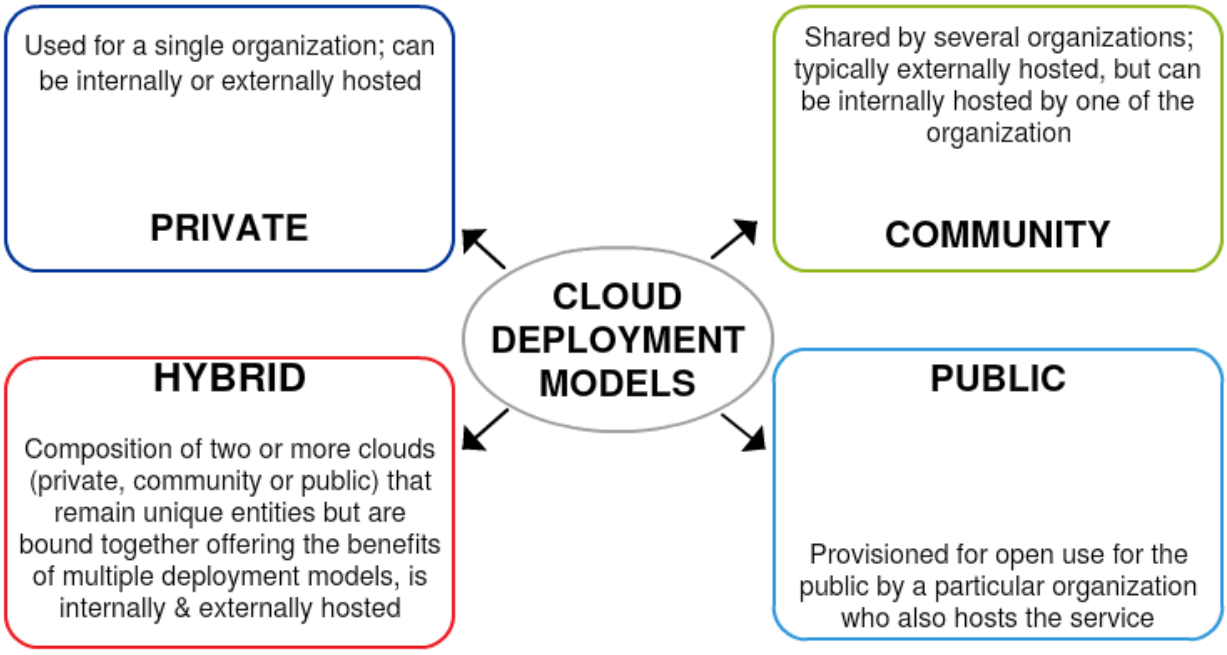
The definition of cloud computing by the NIST identifies four deployment models which are described below in Figure 3.2 (The NIST Cloud Computing Reference Architecture SP 500-292)

(i) Private cloud: Private cloud services are used only by a single company or organization and are not exposed to the public.

(ii) Public cloud: Services of the public cloud are exposed to the public and can be used by anyone.

(iii) Community Cloud: Community cloud services are used by numerous organizations in order to lower costs, as compared to the private cloud.

(iv) Hybrid Cloud: The hybrid cloud services can be distributed in multiple cloud types.



- Figure 3.2 Cloud Computing deployment models. Sources: Yeang *et al* (2016).

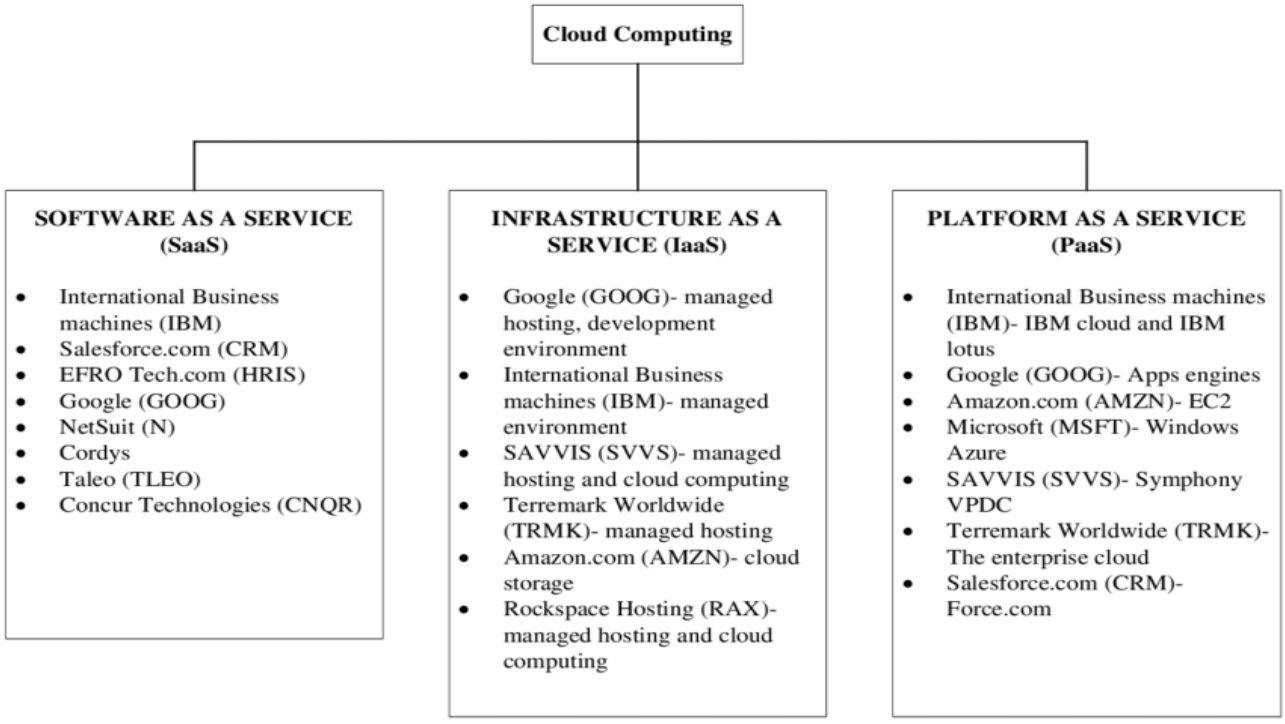
3.2.3.2 Service Models

The definition of cloud computing by the NIST identifies three service models which are described below in Figure 3.3 (The NIST Cloud Computing Reference Architecture SP 500-292)

(i) Software as a Service (SaaS): In SaaS, the user is able to use applications running on the cloud which provides by the cloud provider. These applications are accessible from various machines over the Internet. The user does not control or manage the primary cloud infrastructure involving servers, storage, network and operating systems. Example of the SaaS is storage service such as SkyDrive, Google Drive, and Dropbox.

(ii) Platform as a Service (PaaS): In PaaS, the user can deploy on the cloud infrastructure applications produced using programming languages and tools supported by the cloud provider. The user does not control and manage the primary cloud infrastructure involving servers, network, or storage, but has control over the deployed applications. Example of the PaaS is Windows Azure from Microsoft and Google App Engine from Google.

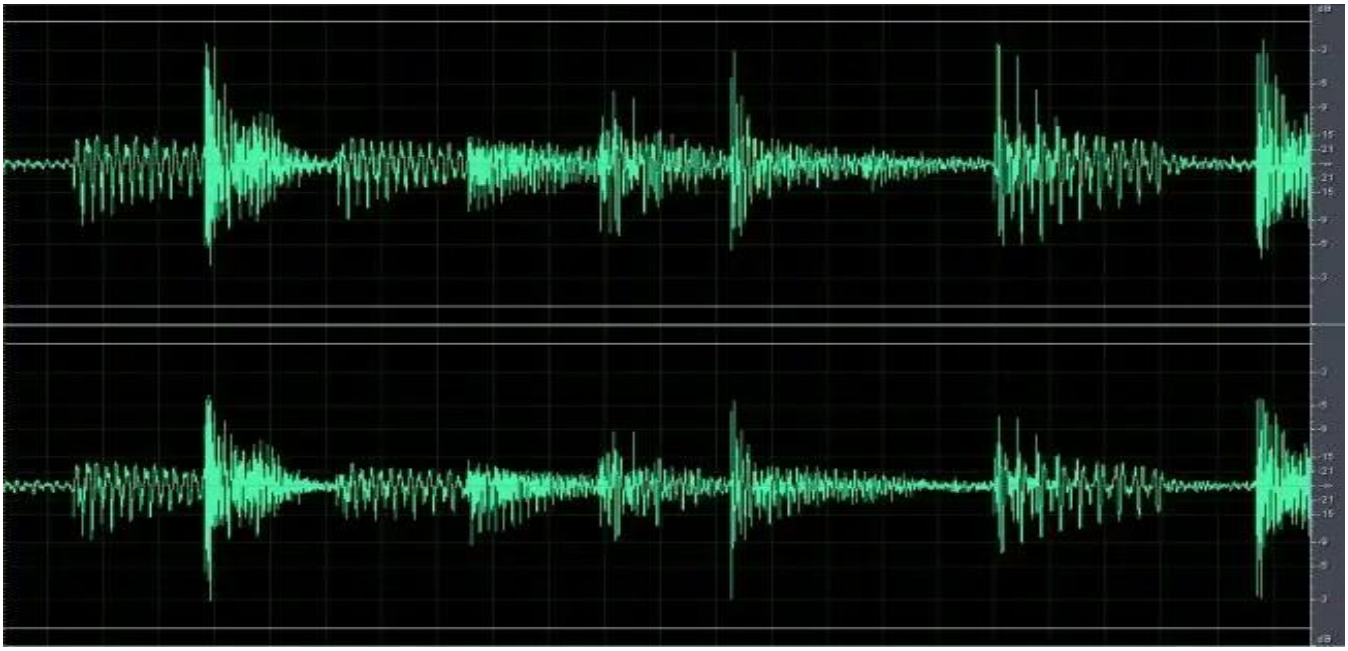
(iii) Infrastructure as a Service (IaaS): In IaaS, the user can provision cloud resources such as network, processing, and storage. Also, the user can deploy and run software which can involve operating systems and applications. The user does not control or manage the principal cloud infrastructure but can control applications, storage, and operating systems. An example of IaaS is Amazon EC2 service.



- Figure 3.3 Cloud Service Models. (Source: Malik et al 2015).

3.2.4 Digital video, audio and photo forensics

Digital video and photo forensics are grouped for a reason. A photo is a still image, and a video is a sequence of still images. When you watch a video, it is a sequence of still mages changing so fast that it appears as continuous movement. If you watch fine minutes of television, you are actually watching thousands of still images changing so fast that the human eye cannot comprehend the individual slides. Digital video and photo forensics are the enhancement and analysis of these individual slides. The primary difference between video and photo forensics is that with a photo, you would enhance them one at a time, and with a video, you might enhance a thousand at a time. Audio forensics is the speciality field of acoustics and audio engineering that deals with the acquisition, analysis, and evaluation of audio recordings that are to be presented as evidence in an official inquiry or a court of law (Maher, 2009:20). Audio forensics consists of the enhancement and analysis of audio recordings created with any type of digital recording device. Audio forensics can be used to verify the integrity of audio recordings or to show that an audio recording has been tampered with (Maher, 2009:20). If a recording is of poor quality, it can also be used to enhance the audio track so that voices become more legible, or background noise that is of interest could be more easily heard (Maher, 2009:20). It is also possible to perform voice pattern recognition with specialized forensic software. These software programs allow for the possible identification of voices with particular people within an audio recording. The figure below shows an example of a forensic audio recording, with manual annotation, displayed with a sound software package.



- **Figure 3.4:** An example of a forensic audio recording. Source: Lastest forensic Science Technology, Rankred.com

The recording depicts the amplitude vs. time waveform of approximately one minute of audio recorded at an emergency dispatch center and includes utterances from the land mobile radio system and the local voice of the dispatcher. Maher (2015:23) asserts that in addition to the analysis and interpretation of tangible audio recordings, audio forensic may also treat questions of audibility in the context of litigation or criminal prosecution, such as civil annoyance complaints from an outdoor performance venue, noise levels produced by take-offs and landings at an airport that violate local statutes, or whether or not a scream or other sound was likely to have been detectable under the circumstances claimed by an ear witness. Forensic acoustics experts who deal with recorded evidence are most often consulted about three concerns: authenticity, enhancement, and interpretation (Maher, 2009:45). Authenticity denotes the acceptance of a recording as being unaltered and true to its source and chain of custody. Criminal and civil cases may hinge on a dispute about the circumstances under which a recording was made and whether audible material in the recording could have been deleted, added, or otherwise

edited after the fact (Koenig, 2007). Musialik and Hatje, (2011:70); Koenig, Lacey and Killion, (2007:252) reveal that forensic audio enhancement involves signal-processing techniques that attempt to improve the intelligibility of speech, the clarity of specific background sounds, or the overall signal-to-noise ratio of the recording. Modern enhancement techniques use a high-quality digital copy of the original recording so the original recording medium is used only to obtain the working copy for enhancement. Interpretation refers to the description of the acoustical evidence in words, pictures, statistics, and graphs that help address investigative questions explain the sequence of acoustical events, and educate the attorneys, defendants, judges, and juries about the meaning, significance, and limitations of the recorded evidence (Audio Engineering Society, 2013; Maher, 2009:43). The figure above depicts an interpretive annotation that has been added to a time waveform to assist with an investigation. Maher (2015:24) claim that, since the 1960s, the use of audio forensics as a collection of techniques to provide scientific evidence relating to audio recordings has been utilized and although technology, the types of crime, and the methods of investigation have changed and the fundamental methodology behind forensic audio remains the same: -

(a) Obtain an audio recording pertaining to a crime
(b) Perform scientific analysis of the recording
(c) Compile a report based on the analysis

Maher (2015:24) further adds that the courts in the United States (US) have generally begun to accept the unique importance of audio recordings, especially in cases involving speech obtained via clandestine surveillance or wiretaps, there were significant considerations regarding the US Fourth Amendment's protections against unreasonable searches and seizures and concern about the legal admissibility of a recording as being a bona fide representation of the sonic events actually present during the recording process. Among the key cases in the US federal court system regarding the admissibility of audio forensic evidence is *United States v. McKeever* (1958). The judge in the Mckeever case was asked, for the first time, to determine the legal admissibility of a tape recorded conversation involving the defendant. The judge ultimately allowed in court the use of a written transcript of the recorded conservation. The Mckeever ruling is particularly important because the judge cited seven specific requirements necessary for a recording

to be accepted in court and those requirement are now assumed by most state and federal courts in the United (States *United States v. McKeever*, 1958):

(a) That the recording device was capable of taking the conversation now offered in evidence.
(b) That the operator of the device was competent to operate the device.
(c) That the recording is authentic and correct.
(d) That changes, additions or deletions have not been made in the recording.
(e) That the recording has been preserved in a manner that is shown to the court.
(f) That the conversation elicited was made voluntarily and in good faith, without any kinds of inducement.
(g) That the speakers are identified.

Since the early 1960s, US Federal Bureau of Investigation (FBI) laboratories have developed techniques and procedures for assessing the authenticity and audible contents of forensic audio recordings obtained from law enforcement investigations, and similar capability has been instituted in other public and private forensic acoustics labs around the world. According to Maher (2015:24), a significant turning point in the practice of forensic audio in the United States occurred 15 years after McKeever during the Watergate scandal. In 1971, late in his first term in office, President Richard Nixon directed the Secret Service to install audiotaping systems in the Oval Office and the Cabinet Room of the White House, in the president's private office in the Executive Office Building (EOB) next to the White House, and at Camp David, the president's retreat in rural Maryland. The existence of these recording systems was known only to a select group of individuals and to the Secret Service (Nixon Presidential Library & Museum, 2015). President Nixon presumably assumed that the recording system's existence would be of interest to no one other than presidential biographers and historians after he left office. However, it quickly turned into a political and legal bombshell of historic proportions in 1973 when White House aide Alexander Butterfield revealed during his congressional testimony that there were secret audiotape recordings of conversations between the President and his advisors! After all, this was in the midst of the Watergate investigation and the widespread public concern about the veracity of various White House officials

who had testified before Congress and in federal court. President Nixon eventually agreed to release edited transcripts of the various conversations recorded by the secret taping system and later the tapes themselves (Nixon Presidential Library & Museum, 2015). Many digital audio recording and storage systems incorporate metadata in the digital file format. Metadata may include information about the recording settings, date and time, manufacturer of the device, and its software version. Although metadata can potentially be altered to conceal tampering with the audio data contained in the file, an audio forensic examiner should always review the metadata as part of an authenticity investigation (Koenig & Lacey, 2014).

3.3 COMPUTER FORENSIC TOOLS

The credibility of an expert witness may be crucial to the outcome of a case. If the integrity and credibility of a Police Officer investigating and providing prosecution evidence in a crime are placed in doubt then the prosecution case may fail. Integrity and confidence in the process and the person may be the definitive factor in determining the success or failure of an investigation and prosecution. There are a number of forensic computer software tools of varying sophistication. There is no single point of analysis to assist investigating personnel in their decision as to the appropriateness of a tool to a specific need (Anson with Bunting, 2012). Digital devices at the scene are the most important source of evidence if an incident occurs. Investigators are using digital forensics to extract digital evidence from electronic devices. Today, digital forensics plays a critical role in investigations. The broad use of digital devices in daily life activities makes them an important source of information about people, thus causing them to become a strong potential source of evidence. Digital forensics typically follows a four-step process, which includes: acquisition, identification, evaluation, and presentation (Anson & Bunting, 2012). Nowadays, investigators typically use multiple computer forensic tools during their investigation process to verify their findings and cover all possible evidence items and a report must be written by the forensic examiner to illustrate the findings from a digital forensics examination (Anson & Bunting, 2012). To perform computer forensic tasks, one needs software tools to gain access, and uncover information that is not visible such as files that are deleted, stored in slack space or unallocated space, and files that are hidden

or encrypted (Anson & Bunting, 2012). Furthermore, many tools may be needed to perform investigative tasks such as forensic imaging, searching, documenting, decrypting and much more, which are needed to critically, and correctly. With many computers forensic software tools, such as FTK, ProDiscover, iLook, and EnCase, log files and reports are generated when performing an investigation. Casey *et al* (2018:48) explained that although these forensic software reports illustrate what, and where evidence is found, it is the examiner's responsibility to explain the significance of the evidence recovered and define any limitations or uncertainty that applies to the findings. Some of the computer forensic tools that generate reports are Forensic Tool Kits (FTK), EnCase and ProDiscover. These tools were examined because of their wide use in virtual or digital investigations, and their availability to the researcher. Some computer forensics tools are developed for use by law enforcement only, such program is iLook.

3.3.1 iLook

This is one of the more well–known law enforcement-only forensics tools. It was developed by Elliot Spencer and then maintained by the Internal Revenue Service Criminal Investigation Division (IRS-CI). Its capabilities include imaging, advanced email analysis, and data salvaging or recovering files that have been deleted by the user. This tool is used by law enforcement agencies, and government intelligence agencies and is not available to the general public.

3.3.2 AccessData Forensic Toolkit (FTK version 7.4)

The FTK version surveyed in this research was 7.4 FTK contains a full suite of password recovery tools, drive and media wipers, a registry viewer and other useful products. Although FTK 7.4 comes with its disk imaging software, it can read the images produced by Encase, Linux DD, SafeBack (up to version 2.0), SMART .s01 and others. FTK can generate reports in different formats like (.xml, .rtf, .wml, .docx). FTK reports include exported files, custom logos, and external information such as hash lists, search results, and password lists. FTK produces an XML report detailing all the digital evidence items

that were bookmarked during the investigation process. A simple XSL style sheet is provided to present this information in a clear and readable manner, and the style sheet can be customized to reflect an investigator's data needs.

3.3.3 ProDiscover Forensic Tool (version 5.5)

ProDiscover offers forensic examiners an integrated Windows application for the collection, analysis, management, and reporting of computer disk evidence. ProDiscover version 5.5 forensic edition, supports all Windows-based file systems including FAT 12/16/32 and NTFS Dynamic disks in addition to file systems such as SUN Solaris UFS and Linux Ext 2/3. ProDiscover.v5.5 is completely scriptable using the ProScript interface, and Perl. ProDiscover enables practitioners to locate data on a computer disk while protecting evidence, and creating evidentiary quality reports for use in legal proceedings (ProDiscover, n.d.)

3.3.4 EnCase Forensic Tool (version 6)

EnCase is a software developed by a company called Guidance Software. It is one of the most common tools used in computer forensics. In this research, the researcher also reviewed EnCase version 6. EnCase has an organized user interface that simplifies the viewing of media content using different views. These views include a picture gallery, image evidence, hex, and file tree views. EnCase can also be used to acquire evidence and provides investigators with tool to conduct large-scale investigations from beginning to end. EnCase has several automatically generated reports that can be created by listing all files and folders in a case, a detailed listing of all URLs and corresponding dates and times that websites were visited, document incident report that helps create the required documentation relevant during the incident response process, detailed hard drive information about physical and logical partitions.

3.4 VIRTUAL CRIME SCENE

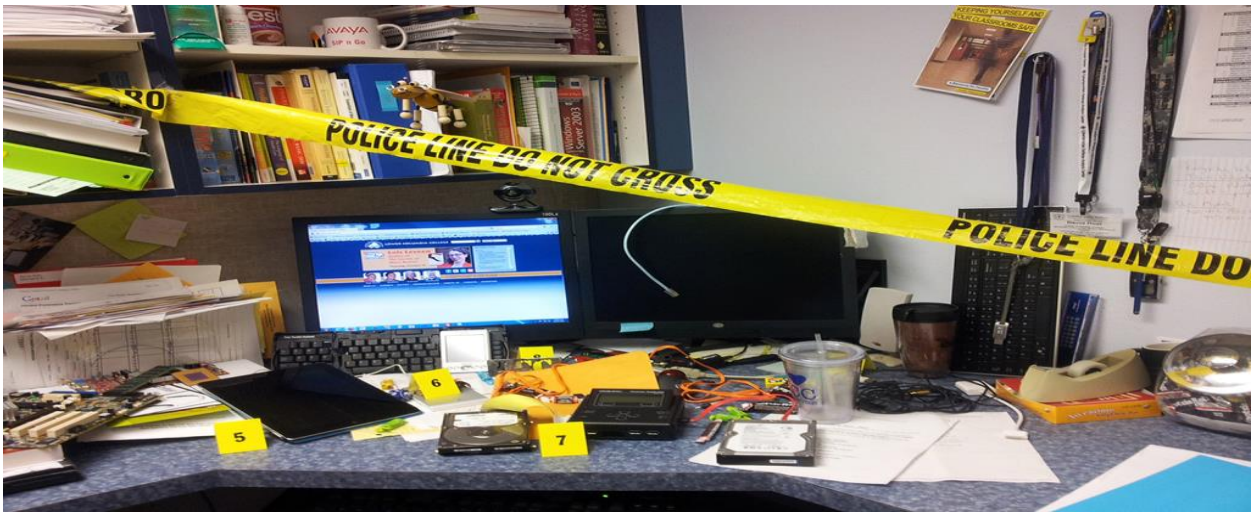
Casey (2011:46) states that computer crime scenes present the technical details that are essential in understanding the exact aspects of computer evidence. When one comes across a computer or any type of computer equipment at a crime scene, it is essential to keep in mind not to be in a hurry because a computer investigator's crime scene is probably wider than that of the traditional investigator. Computer forensic experts should be consulted to analyse and locate pertinent data, for the case to be proper and legal. A computer crime scene has different standards compared to that a traditional crime scene. Crime Scene Investigator Network (2012) states that the goals and objectives of investigating a computer crime scene are the collection, preservation, packaging, transportation and documentation of physical evidence left at the scene. Eoghan (2012:106) claims that when a full investigation is warranted the first challenge is to retain and document the state and integrity of items digital or physical at the crime scene. Protocols, practices, and procedures are employed at this critical juncture to minimize the chance of errors, oversights, or injuries. Whoever is responsible for securing a crime scene, whether first responders or digital evidence examiners, should be trained to follow accepted protocols. Crime scene investigation is more than the processing or documentation of crime scenes (Eoghan, 2012: 227). A crime scene can also be defined as the apex of an inverted pyramid that expands to encompass the investigation of a crime; the recognition, analysis and interpretation of evidence and finally a court trial. However, Eoghan (2012:107) opines that preventing people from disturbing a single computer or room is relatively straightforward but, when networks are involved, a crime scene may include sources of evidence in several physically distant locations.

Assuming investigators can determine where these locations are, they may not be able to reach them to isolate and preserve associated evidence. Barry (2012:64) posits that the application of science and technology plays a critical role in the investigation and adjudication of crime in our criminal justice system. But before science can be brought to bear on evidence, it must be recognised and collected in an appropriate manner at the crime scene. Ross & Donna (2019:1) further add that crime scene processing is an inherent task and duty associated with most criminal investigations, for rarely does one encounter a crime without some kind of crime scene. Crime scene processing consists of an examination and evaluation of the scene for the express purpose of recovering digital

or physical evidence and documenting the scene's condition *in situ,* or as found (Ross & Donna, 2019:64). The end goal of crime scene processing is the collection of the evidence and scene context in as pristine a condition as possible. To accomplish this, the crime scene investigator engages in six basic steps such as assessing, observing, documenting, searching, collecting, and analysing (Ross & Donna, 2019:20). These steps and the order in which they are accomplished, are neither arbitrary nor random. Each serves a purpose in capturing scene context and recovering evidence without degrading the value of either.

It is very important "to be aware, as an investigator, of considering several points when dealing with the crime scene. The scene of the crime may not be the actual location of the crime, but also the staging and planning area. It may be the initial place where the crime was planned or ended. Yet, from these efforts, the crime scene investigator will walk away with important items of digital or physical evidence and scene documentation in the form of sketches, photographs, notes, and reports. All this information plays a significant role in resolving crime by providing objective data on which the investigating team can test investigative theories, corroborate or refute testimonial evidence, and ultimately demonstrate to the court the conditions and circumstances defined by the scene. Action without purpose is folly and, simply put, becomes a wasted effort. This is true in any endeavour. Therefore, it is imperative that before pursuing the actions a crime scene investigator conducts at the scene, they must understand their mandate. The scene of the crime is not where information can be collected from witness and victim but also digital and non-digital evidence that could assist in the prosecution of the crime can be found and Information in the form of non-digital or physical evidence needs to be photographed for record keeping. According to Fisher (2012:46) crime scene is the place where the crime was committed, and where physical evidence associated with the crime may be tracked down. Analysis of the scene of the crime is a distinctive concept in forensic science. The evaluation of crime scene investigation involves for instance the context of the scene, and evidence extracted to identify the occurrence and order of sequence. Crime scene investigation is a dynamic process that requires an active approach by the investigator, who must be aware of the linkage principle of the evidence and must use crime scene analysis methods and techniques in order to offer an opinion

on the reconstruction of the crime. Computers, mobile devices, and networks are considered as an extension of the crime scene, even when they are not directly involved in facilitating the crime, as they can contain useful information and provide a digital dimension. A virtual crime scene can contain many pieces of evidence and it is necessary to apply forensic principles to survey, preserve, and document the entire scene. Egohan (2012:227) justified that a single computer can contain e-mail communications between the victim and offender, evidence of intent to commit a crime, incriminating digital photographs taken by the offender as trophies, and software applications used to conceal digital evidence. Figure 3.5 Depicts crime scenes involving Computer Systems.



- Figure 3.5 Depicts crime scenes involving Computer Systems. Source: Computer & laptop repair services in columbia, SC.

3.5 CLASSIFICATION OF CRIME SCENES

James, Bell and Nordby (2014:167) state that crime scenes are classified according to the location of origin of the initial criminal activity. The classification of the crime scene labels can be either a primary crime scene or a secondary crime scene.

3.5.1 Primary crime scenes

Swanson, Chamelin, Territo and Taylor (2019:59) state that the location where the initial offence was committed is termed as the primary crime scene. This includes the entry and exit points used by the suspect. Palmiotto (2013:164) supports Swanson *et al* (2019:60), explaining that a primary crime scene is a location where the body of a victim is found or the point of entry or exit. Simply put, it is the scene at which a crime or event has taken place. Any adjacent areas with evidence, or with the sign of forced entry are also a part of the primary scene.

3.5.2 Secondary crime scenes

A secondary crime scene is a place or location where some of the victim-offender interaction occurred but is not the actual place where the offence occurred (Turvey, 2012:291). The secondary crime scene is the location used by the perpetrator for surveillance of victims and planning the crime. These are areas where physical evidence relating to the crime may be found and these areas consist of the vehicle or other conveyance used to transport the evidence, areas where the perpetrator may have cleaned up after the incident and areas where the perpetrator discarded tools or weapons or other items and the area where initial contact between suspect and victim and or the assault occurred.

3.6 PROCESSING THE DIGITAL CRIME SCENE

Ross and Donna (2019:1) posit that crime scene processing is an inherent task and duty associated with most criminal investigations, for rarely does one encounter a crime without some kind of crime scene. Crime scene processing consists of an examination

and evaluation of the scene for the express purpose of recovering electronic or physical evidence. Casey (2011:245:) contends that virtual crime investigations are generally messy and complicated because of the extreme emotions, concealment behaviour and various types of evidence involved. These investigations require a methodical approach to ensure that all relevant items are recognised, collected, and examined properly. Given the scope and consequences of violent crimes such as rape and homicide, it is advisable to seek out and preserve all available digital evidence-not just what is proximate to the crime scene. In addition, the offender may have taken steps to conceal incriminating data or misdirect the investigation. Provide the proper authorization is obtained, digital evidence searches can include the victim's and suspect's home and workplace, and other places they frequent. Given the amount of effort involved, it is generally necessary to have a team working together to preserve all of the digital evidence related to a violent crime.

3.7 VIRTUAL CRIMINAL INVESTIGATION APPROACHES AND CHALLENGES

Virtual Criminal Investigation has become a predominant field in recent times and courts have had to deal with an influx of related cases over the past decade. As computer or cyber-related criminal attacks become more predominant in today's technologically driven society and there is the need for and use of, digital evidence in courts has increased. There is an urgent need to hold perpetrators of such crimes accountable and successfully prosecute them. According to Swanson *et al* (2019), the roots of a criminal investigation can be traced back to England in the eighteenth century a period marked by significant social, political, and economic changes. Criminal justice agents, such as law enforcement officers, prosecutors, and judges, are responsible for the prevention, mitigation, detection, investigation, prosecution, and adjudication of cybercrime.

Successfulness of law enforcement in virtual crime investigations depends on streamlining and strengthening the procedures and also reducing the impediments which hinder how law enforcement conduct investigations. There are two-pronged solutions for effective virtual crime investigations: the criminalization response which was highlighted and addressed in the previous chapter shows that the traditional laws or substantive laws

that were formulated to deal with real-world issues or crimes were insufficient to administer all categories of virtual crime. There has been a suggestion that an effective substantive law is needed. Enacting an effective or comprehensive substantive law is only half of the solution to combating virtual crime. The other half is how is the institution of an effective and efficient investigation approach to virtual crime by investigators. The approach to these requires, first the optimum identification of investigation models and how to respond to the legal challenges that hinder the law enforcement approach or the ability to investigate virtual crime. This section is to streamline the virtual crime investigation process and harmonise policies and procedures designed for virtual criminal investigations. Also, the section will examine the factors necessary for successful investigations, identifying and eliminating legal challenges faced by investigators. It accepts that the approach model to virtual criminal investigation embraced by the Ghanaian Cybercrime Unit does not have enough of specified methods or steps of the investigation approach. Therefore, some of the formulated methods, protocols and models of cybercrime investigation by the United States (US) Department of Justice, Australian High Tech Crime Centre and Indian Cyber Crime Coordination Centre (I4C) and by experts in computer forensics will be analysed and compared with the Ghana investigative approach.

So far the government of Ghana has shown seriousness in embracing Information and Communication Technology. In June 2003 Ghana Government introduced and signed a policy document on Information and Communication Technology for Accelerated Development (ICT4AD) (Ghana ICT for Accelerated Development Policy, 2003). Nations worldwide have recognized the developmental opportunities and challenges of the emerging information age characterized by information and communication technologies (ICTs). These technologies are driving national development efforts worldwide and a number of countries in both the developed and developing world are exploring ways of facilitating their development process through the development deployment and the exploitation of ICTs within their economies and societies (Ghana ICT for Accelerated Development Policy, 2003). The Ghana ICT for Accelerated Development (ICT4AD) Policy represents the Vision for Ghana in the information age. The development of this policy framework was based on a nationwide consultative process involving all key

stakeholders in the public sector, private sector and civil society. Also, in 2014 the government of Ghana set up a national Computer Emergency

Response Team (CERT) to address all cybersecurity-related crimes and problems and will also work to halt internet fraud (Sakawa) and stop the abuse of children online in Ghana and report to the Ghana Police. CERT-GH coordinates security incidents on behalf of its constituency and has no authority to reach further than that. By so doing, the government has empowered the Ghana Police Service to set up the Cybercrime Unit to review and propose Investigation methods, policies, laws, regulations, guidelines and standards on the management of electronic crime or cybercrime in Ghana.

Computer Emergency Response Team (CERT) is a unit or department at the National Cyber Security Centre under the Ministry of Communications a public organisation in charge of Communications. The Computer Emergency Response team play a vital role in thoroughly evaluating, applying, and monitoring criminal activities of online offenders but the Ghana police service cybercrime Unit is assigned to investigate virtual criminal cases and gather information, including searching for and seizing both physical and electronic evidence, labelling the crimes, and standing before the court of law to prosecute the offender. Since the establishment of the Ghana Police Cybercrime Unit, there have been remarkable advances, intended to overcome investigative challenges and keep abreast of Information and Communication Technology. This has led to the growth of an efficient department within the Ghana Police Service and in the appointment of specialised criminal investigation officers and detectives dealing with specialised crimes. In recent years, for example, the Ghana government has assisted the Ghana Police Service to establish a number of departments, such as the Forensic Science Laboratory which provide scientific support to criminal investigations with respect to digital evidence analysis (Ghana Police Service, 2022). For this purpose, the Ghana Police Cybercrime Unit has put together but not having enough guidelines for the procedure to be followed in dealing with the virtual crime scene and digital crime evidence.

3.8 VIRTUAL CRIME SCENE PHOTOGRAPH AND VIDEOGRAPHY

Documentation of the crime scene is truly the most critical element of scene processing (Ross & Donna 2019:107). Ross and Donna (2019:108) further assert that without good documentation, it is often difficult to explain or make understandable to a jury any observation made by the crime scene investigator. Without good documentation, it can be difficult if not impossible, to respond to a well–thought–out cross-examination. If there is no supporting documentation that clearly and concisely demonstrates the points the crime scene investigator is trying to make, counsel will effectively argue that the Crime scene investigator (CSI) is mistaken. Crime scene documentation element includes notes, photographs, videography, sketches, and report. For the purpose of this research, the researcher is less concerned with the technical aspect of photography, which certainly is important. The figure below depicts Polaroid studio series marco ring light for crime scene investigation.

- Figure 3.6 Depicts NIKON D7100 24.1 MP DSLR. 24.1 MP stands for 24.1 megapixels digital single-lens reflex camera.

The greatest benefit of having a camera with a high megapixel rating can be captured in greater detail. The greater the number of megapixels, the higher the definition of the image reproduces, and the larger size an image can be printed and will retain sharpness and detail.

- Figure 3.7 depicts polaroid studio series marco ring light.

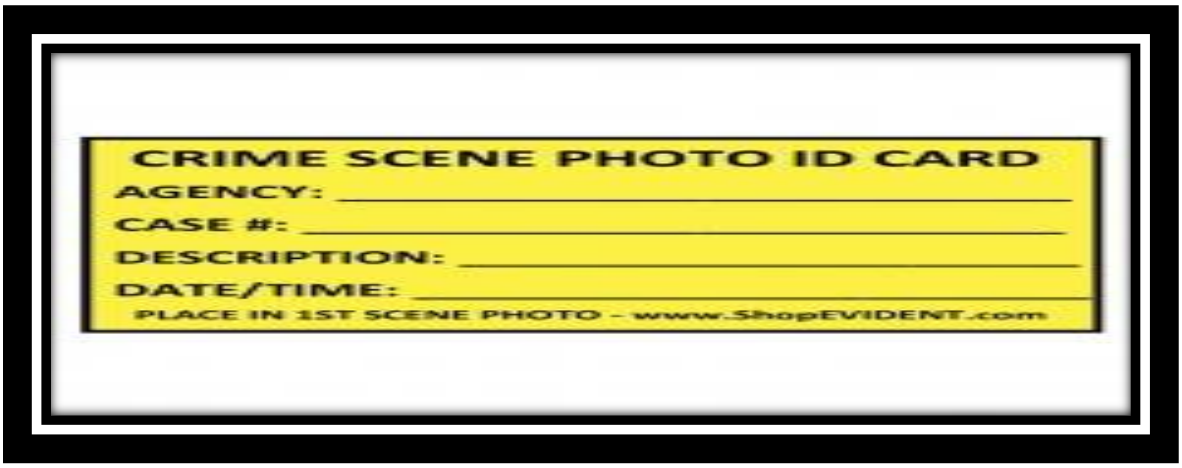
A ring light is designed to give an equal, shadowless source of light on the object being photographed. The light output can be controlled by using only half of the LEDs in the ring light and then rotating, the lights provide some shadow effects if needed. Orthmann and Hess (2013:46) state that "a picture is worth a thousand words". Orthmann and Hess (2013:50) state further that the CSTS must take sufficient photographs to reconstruct the entire scene. Throughout the multiple disciplines of forensic science, and the many topics that fall under the discipline of forensic science, every section had one activity in common. Gardner and Bevel (2009:249) maintain that a crime scene is preserved in images, sketches, notes and physical evidence – each of which serves its unique function in preserving the scene. Gardner and Bevel (2009:249) add that although the crime scene itself no longer exists, the goal is to preserve it in such a way that it can be understood and virtually reconstructed if needed. Forensic photography plays a very critical role in investigation. Pepper (2010:30) states that photography is the recording of an image onto a light-sensitive film or an electronic sensor. Forensic photography entails the recording and documenting of items of physical evidence found at the crime scene, using a camera,

in the same setting or conditions in which they were found by the investigator (Fisher 2012:79). It provides a permanent record for the courts (Miller with Massey, 2016:49). Pepper (2010:30) supports the views of Fisher (2012:79) and Miller and Massey (2016:49), stating that whether the evidence is located inside or outside, during the day or night, and irrespective of the weather conditions, the photographs taken must be an actual, accurate, permanent record of the evidence as it was found. Forensic photography includes methods of photographing the scenes of crimes, gunshot wounds, bite marks, weapons, trace evidence and autopsy procedures. Vernon, (2015:191) indicates that the use of digital video recording has become increasingly popular and has been employed over the years with excellent results in the investigation of virtual crime, homicide and other crimes. Robinson (2016:550) further reveals that the digital video camera is a device that records video in different formats such as Digital8, MiniDV, Digital Video Disk (DVD), an SD card, a mini SD card, a Hard drive, or solid-state flash memory. A video is also a great tool for underwater criminal investigators and photographers (Robinson, 2016:550). The use and availability of digital video recorders to enhance this documentation is an excellent medium because many people who have smartphones with high–resolution video capabilities and camcorders in their homes are aware of video and videotaping (Vernon, 2015:191). A digital video recorder captures 30 frames of video per second. This complements the human eyes' persistence of vision, constantly keeping the viewer informed as to direction and perspective even though the lens may be moving and its field of view is continually recording differing angles of view. An entire crime scene can be scanned and captured in great detail. In addition, items that may have been missed originally will still be preserved on tape.

3.8.1 Crime Scene Photography and the Investigator

To say that a picture is worth a thousand words is true in terms of understanding a crime scene (Ross & Donna, 2019:107). The investigator should have a basic understanding of photography and be able to operate some of the more simple photographic equipment

available today. An easy-to-use camera should be provided for use by the investigator at the virtual crime scene. Digital cameras as well as shoot cameras and many of the iPhone models are simple to operate and ideal for obtaining a record of the crime scene and any changes that occurred. One way an image can be established as being a photograph from a particular crime scene is to have the photographer who took the image testifies in court. Photographers can state they took the photograph, what the subject matter of the image was supposed to be, where it was taken, and when it was taken. Robinson (2016:62) opines that the photographer or the investigator should be able to testify about the camera and flash variables used to capture the image and defend this choice if necessary. Robinson (2016:62) also posits that the photographer's first image on every crime scene should be of a Photo Identifier. Although variations of identifiers are used by different law enforcement agencies there are some common elements that exist in most of them. Figure 3.8 shows a typical example of a photo identifier for crime scene photography.



- **Figure 3.8** shows a typical example of Labelled scale for crime scene photography. (Source: Shop Evident)

Robinson (2016:63), opine the following as the basic information that should be included on the photo identifier:

(a) The case number: the case number is preferred to the crime type because the crime type may change between the time of the initial call

that reported the incident and the type of the case that is going to court. Incident types may change for many reasons. The seriousness of the case may go up in severity. A case originally reported as "shots fired" may subsequently end up in court as a homicide prosecution. The seriousness of the case may be revised downward. The initial report of a "rape case" may end up in court as a simple assault because of plea bargaining. However, the case number does not change.

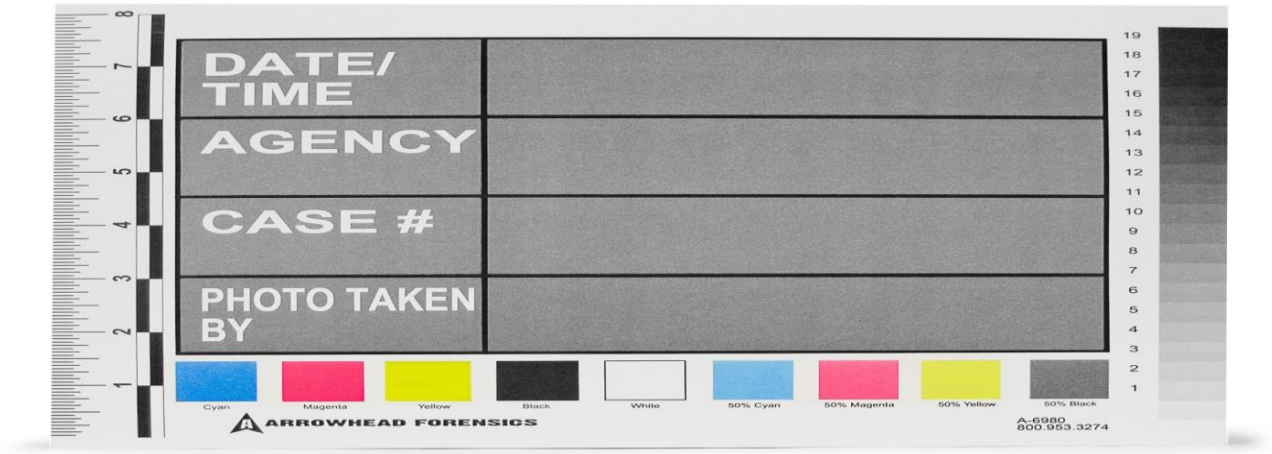
(b) The date when the first image was taken. Many agencies also include the time the first image was captured and of course, the image should be the photo identifier

(c) The address or location of the photographs. Most frequently this is a street address. Sometimes the name of the business is also included. For example, First Allied Bank, 28th Augustus Street. If a particular room or suite number is applied add this also.

(d) The name of the photographer. Initials badge numbers or employee identification numbers should be used also

(e) Some agencies include the model of the camera and also indicate the digital flashcards which are currently being used.

Robinson (2016:65) further contends that each item of evidence should include several closed – Up Photographs. It is standard practice to include a Labelled Scale in at least one of the close-up photographs. A labelled scale can be a pre-printed form, or it can be as simple as a 6 ruler with a removable label on it. Labelled scales are predominantly grey, scales come in a variety of colours such as black white, grey, fluorescent, and transparent. A typical example of Labelled scale for crime scene photography is shown below.



- Figure 3.9 depict Labelled scale for crime scene photography (Source: Arrowhead Forensics)

3.8.2 The Value of Crime Scene Photographs and Video recording

According to Robinson (2019:128), the purpose of photography is to do the following:

(a) Provide a permanent record of the place and position of objects and physical evidence found on the crime scene, for future use and reconstruction purposes.

(b) Convey the crime scene and circumstances of the crime to a jury and serve as visible evidence and provide a new slant on the case

(c) Pictorially provide a visual record and representation of the crime scene and related areas.

(d) It provides a more realistic and graphic portrayal of the virtual crime scene:

(e) It tends to capture the atmosphere of the scene, especially when the investigator is narrating the events as they are being depicted on film.

(f) Refresh the investigator's memory and recall significant details that may have been overlooked or forgotten and review a particular aspect of the case

3.9 VIRTUAL FORENSIC INVESTIGATIONS PROCESS AND MODELS

Casey (2011:187) argues that to make the most of digital evidence, forensic practitioners need to understand, and make regular use of, the scientific method. The scientific method applied in conjunction with digital forensics methodologies and techniques enables us to adapt to differing circumstances and requirements and to ensure that conclusions reached are solidly based on fact. Casey (2011:187) advocates that the forensic analysis process involves taking factual observations from available evidence, forming and testing possible explanations for what caused the evidence, and ultimately developing a deeper understanding of a particular item of evidence or the crime as a whole. Put another way, elements of digital forensic analysis include separating particular items for individual study, determining their significance, and considering the entire corpus of evidence.

Du (2020:19) indicates that the first digital forensic process model proposed contains four steps: Acquisition, Identification, Evaluation and Admission. Du (2020:20) reveals that numerous process models have been proposed to explain the steps of identifying, acquiring, analysing, storing, and reporting on the evidence obtained from various digital devices.” In recent years, an increasing number of more sophisticated process models have been proposed. These models attempt to speed up the entire investigative process or solve various problems commonly encountered in forensic investigation. Scanlon *et al* (2017:573) contend that the diversity of devices and sources of digital evidence results in a corresponding diversity in digital forensic process models. According to Scalon *et al* (2016:10), there is no single, universal process model suitable for all types of investigation. Reducing the volume of data for arduous, manual analysis will speed up the entire investigative workflow and can significantly aid in alleviating digital forensic backlogs. In digital forensics, a process model is a methodology to conduct an

investigation; a framework with several phases to guide an investigation. Generally, process models were proposed on the experience of previous work. Due to the variety of cases, e.g., cyberattacks conducted by IT specialists, civil cases in a corporation, or criminal cases, different investigators tend to follow different methods in their investigative process, there is no standard workflow in digital forensic investigation (Du, Le-Khac, & Scanlon 2017:573).

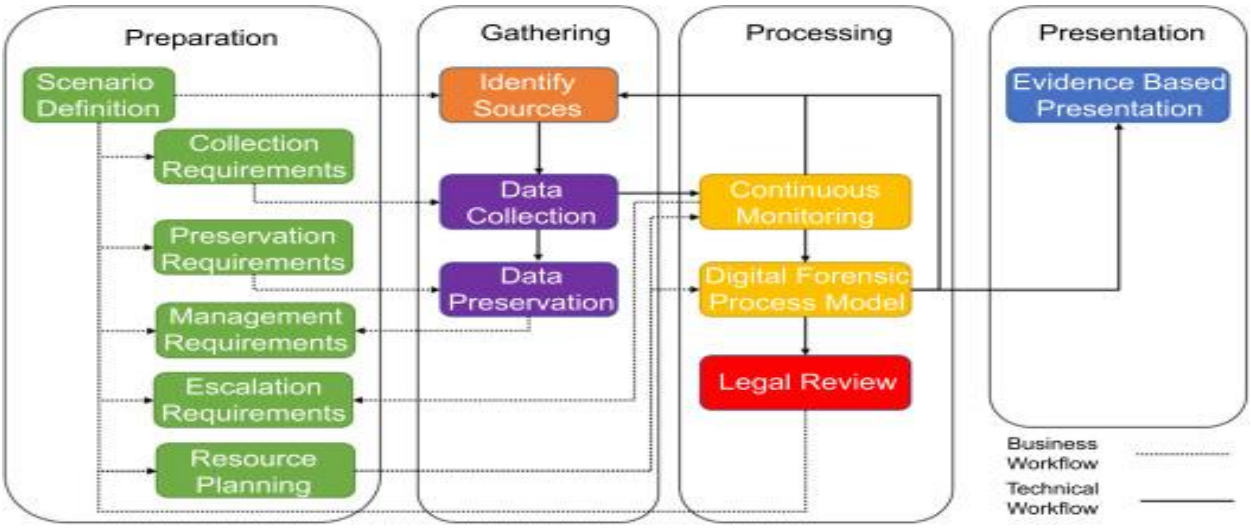
The traditional framework had been refined and formed a number of novel frameworks. Some inheritance relations among the existing frameworks are listed below:

(a) DFRWS model (Palmer, 2001) → SRDFIM (Agarwal, Megha, Saurabh & kumar 2011)
(b) DFRWS model (Palmer, 2001) → An Abstract Digital Forensics Model (Reith, Carr & Gunsch 2002)
(c) IDIP (Carrier and Spafford 2003) and DCSA (Rogers 2006) → Triage Peocess Model CFFTPM (Rogers, Goldman, Mislan, Wedge, & Debrota 2006)
(d) Integrated Digital Investigation Process (IDIP) (Carrier and Spafford 2004) → Enhanced Integrated digital Investigation Process(EIDIP) (Baryamureeba and Tushabe 2004)
(e) Integrated Digital Forensic Process Model (Köhn, Olivier, & Eloff, 2013) → DFaaS Process Model (van Baar, van Beek, & van Eijk, 2014)

Lee *et al* (2001) proposed a Scientific Crime Scene Investigation (SCSI) model for digital forensic investigation 2001. However, Ciardhu´ain (2013:38) criticises SCSI and reports that the model is not a systematic digital forensic process model because it only focuses on physical crime scene investigation and lack of describing on digital criminal scene investigation. Kohn *et al* (2013:38) argue that the physical crime scene investigation process can be adapted to digital crime scene investigation. An Event-based Digital Forensic Investigation Framework separates the concepts of the physical crime scene

and the digital crime scene, collecting digital devices from the physical crime scene and then obtaining digital evidence from the digital devices' storage.

An Enhanced Integrated Digital Investigation Process (EIDIP) model was proposed by Baryamureeba and Tushabe (2014:102). The EIDIP model is based on IDIP, by introducing a traceback phase to address the problem of having to reconstruct twice in IDIP. Figure 3.10 below is a systematic digital forensic investigation process model.



- **Figure 3.10** Digital Forensic investigation process model.

3.10 VIRTUAL CRIMINAL INVESTIGATIONS PRIORITY AND APPROACHES

The procedures used in the virtual criminal investigation process were developed focusing on particular areas of the electronic evidence acquisition process. Hewling (2013:18) posits that this has resulted in very little regard being made for the core components of the digital forensics field, for example, the legal and ethical along with other integral aspects of investigations as a whole. According to Hewling (2013:44), these core facets are important for a number of reasons including the fact that other forensic sciences have included them, and to survive as a true forensics discipline, digital forensics must ensure that they are accounted for (Hewling 2013:18). This is because;

digital forensics like other forensics disciplines must ensure that the evidence (digital evidence) produced from the process can withstand the rigours of a courtroom. Smith, Grabosky, and Urbas (2012) posit that prioritising certain virtual crime categories for investigations is important because the capability of virtual crime or Cybercrime Units to perform a variety of cybercrime investigations is limited compared to the investigation of traditional crimes. This is for two reasons. The first is because the volume and diversity of cybercrimes have increased significantly in recent years. For example, statistics published in 2005 by the CSI/FBI Computer Crime Survey and the Australian Computer Crime and Security Survey in 2006; foresee a containing increase in the number of complaints and crimes. Secondly, trivial traditional crimes, such as misdemeanours, and traffic violations, need much less time and fewer resources to be investigated. Meanwhile, virtual crimes that are trivia require more investigative resources, such as first responders, technical teams, forensic experts, digital forensic tools, and other equipment commensurate with serious virtual crimes. In many instances, there is a collaborative process of policing cybercrime between law enforcement and members of the community. The community's level of knowledge and awareness of cybercrime may affect their perceived risk of victimisation and knowledge about preserving evidence for investigations and willingness to report incidents (Wall, 2008).

Established literature examines community perceptions of cybercrime and associated investigations. Popular perceptions of cybercrime and the capabilities of police to investigate incidents are shaped by cultural portrayals within the media. There is an erroneous perception, reflected in portrayals of computer hackers in cyberpunk media like The Matrix, Die Hard or Blackhat, that cybercriminals possess mastery over technology (Wall 2008: 863). These texts shape security mindsets that influence expectations of cybercrime investigations (Kremer 2014). Several factors are used to determine when a crime is high-profile or trivial. Law enforcement agencies determine which crime is high profile case or trivial. Chang *et al* (2018); Cross 2018c (550); *et al* (2013: 86) are of the opinion that Social judgements about wrongdoing and past life experiences also influence community perceptions about cybercrime. For example, research suggests that victims and witnesses of cybercrime are motivated to report

incidents by their internal sense of justice and an altruistic desire to protect others from harm.

A few decades ago heinous and violent crimes always had priority over cybercrimes. One takes note that Goodman (1997: 447) opines that, the latter was not a priority for law enforcement or to the mass media worldwide for a number of reasons, among them that internal police culture places a lower value on catching non-violent offenders, and that investigative priority is primarily set according to the scale and significance of the complaints and their physical damage. For example, Ken Hunt, a former Australia Federal Police (AFP) detective superintendent, said: most of my colleagues, most of the other people at my level, thought computer crime was a wank. And that I should be out there investigating "real crime" (Shane, 2006:28). On this situation, Alaeldin (2009:93) states that, there has been a change entirely by the rapid and continuing expansion of cybercrimes, because of the prevalence of cybercrime offences and the establishment of cybercrime Units which have significantly contributed to the positive change in both knowledge and attitude to the seriousness and priorities of cybercrimes. Alaeldin (2009:94) further contends that traditional violent crimes are ranked in seriousness as either felonies or misdemeanours, depending upon the severity of the crime and the maximum punishment that can be imposed. Serious crimes are always placed on the frontline by law enforcement in every jurisdiction. For example in the United States, the 'Quality over Quantity" programme was ordered by Clarence Kelley, the then director of the Federal Bureau of Intelligence (FBI) in 1975 to establish parameters for prioritising traditional crimes. By contrast, different types of virtual crimes are not ranked as felonies or misdemeanours, and therefore, Cybercrime Units must apply internal guidelines, measures, or policies to ensure that serious cybercrimes are investigated immediately (Alaeldin 2009:94).

3.10.1 The Ghana Police Cybercrime Unit

The Ghana Police Cybercrime Unit has not established parameters that specify which cybercrime or virtual crimes are worthy to be investigated. Obuobisa (2019) states that law enforcement institutions in Ghana have inadequate digital forensic tools to gather electronic evidence and investigators and sometimes have to fall on private cyber forensic companies for assistance in conducting digital investigation. It is a fairly new area in our criminal Jurisprudence and so we lack enough precedents to resort to in prosecuting these cases. Improper handling of electronic evidence by investigators is not in compliance with our admissibility rules (Obuobisa, 2019). This leads to very vital evidence being rejected by the courts. Conversely, the Ghana Police Cybercrime Unit investigation team lack skills to prioritize investigations of virtual crimes. Although Ghana has laws that combat and give investigative powers for cybercrime investigations, there is still a need for training security personnel for better approaches to authenticate hardware, software, and data on computer systems and verify user identities and the creation of methods of monitoring and detecting security compromises.

3.10.2 Department of Justice (DOJ) the USA

In the USA, the Cybercrime Unit of federal investigators, State Police, and county sheriffs prioritise cybercrime investigations. They exclude several categories of cybercrimes from their investigations prioritise and focus more on particular types of cybercrimes. The FBI has specially trained cyber squads in each of our 56 field offices, working hand-in-hand with interagency task force partners. The rapid-response Cyber Action Team can deploy across the country within hours to respond to major incidents. For instance, online gambling and cyber prostitution are placed at the very bottom of their list of investigations, meanwhile, virtual crimes such as child pornography, and intellectual property have received much attention from investigators in the USA and have a high priority (Smith, Grabosky & Urbas, 2014). In addition, federal cybercrime units have set three criteria that need to be met before launching an investigation. The first criterion is the magnitude of the pecuniary losses caused by a cybercrime (Stephenson, 2000).

The threshold set is $5000 or more worth of damages or losses caused. According to, cybercrime units in the United States declined to conduct a criminal investigation if the threshold value is not reached; however if the same crime were committed against several victims, the agency accumulates them to reach an amount above the investigate threshold. For instance, if one hundred victims each lost $100; the centre will treat them as a $10,000 case, taking them over the threshold. However, in September 2008 Congress revised the Computer Fraud Abuse Act (CFAA) to give federal prosecutors the ability to use the statute in a wider variety of cases. The amended revision of the statute removed the $5000 requirement from § 1030 (a) (5). The second criterion is that the crime has been committed within the limits of the jurisdiction of the agency. Finally, cybercrime units sketch out a preliminary investigation to determine whether the crime is solvable by studying the scene of the crime (Stephenson, 2000) and prosecutable by applicable USA law (Smith, Grabosky & Urbas 2012).

3.10.3 National Crime Agency (NCA) in the United Kingdom

The National Crime Agency (NCA) leads UK law enforcement's fight to cut serious and organised crime. The National Cyber Security Centre (NCSC) is a part of GCHQ and is the UK's lead authority on cyber security. The National Cyber Crime Unit (NCCU) of the NCA leads the UK’s response to cybercrime, supports partners with specialist capabilities and coordinates the national response to the most serious of cybercrime threats. The NCCU works closely with the Regional Organised Crime Units (ROCUs), the Metropolitan Police Cyber Crime Unit(MPCCU), and partners within Industry, Government and International Law Enforcement. Some of the Functions of the NCCU are as follows:

(a) Providing a powerful and highly visible investigative response to the most serious incidents of cybercrime by pursuing cyber criminals at a national and international level.
(b) Working proactively to target criminal vulnerabilities and prevent criminal opportunities.
(c) Assisting the NCA and wider law enforcement to pursue those who use the internet or ICT for criminal purposes.

(d) Directing a step-change in the UK’s overall capability to tackle cybercrime, supporting partners in industry and law enforcement to better protect themselves against cybercrime.

3.10.4 Australia High–Tech Crime Centre (AHTCC)

In response to the significant challenges presented by cybercrime, the Australian Government launched the National Plan to Combat Cybercrime (Attorney-General's Department, 2013) and Australia's Cyber Security Strategy (Department of Home Affairs, 2020). Cross-jurisdictional characteristics and technical complexity present a distinct challenge for cybercrime investigation by law enforcement (Holt 2018: 143–144). These characteristics have implications for community and police perceptions of cybercrime, including the likelihood that victims will report incidents to law enforcement. Currently, Australian federal and state police agencies refer victims of cybercrime to the Australian Cyber Security Centre's Report Cyber portal. An incident may then be referred back to the state or federal police for an official investigation (Australian Federal Police, 2019; Queensland Police Service (QPS) 2019: para 4). Previous Australian research suggests that general duties officers remain a primary point of contact for victims of cybercrime and that victims are often dissatisfied when these officers refer matters elsewhere (Cross 2020, 2018b: 5–7). This suggests that discrepancies between community and police expectations about appropriate responses to cybercrime may contribute to public dissatisfaction with law enforcement (Cross *et al* 2016; Jang *et al* 2010).

Less is known about Australian law enforcement's ability to investigate technologically sophisticated cybercrimes, including those involving the use of cryptographic technologies such as public key encryption, onion routing and cryptocurrencies. This problem of digital communications 'going dark' to police surveillance enables cybercriminals to mask their real-world identities and locations (Weimann, 2016). General duties officers broadly lack the skills necessary to investigate offences involving such technology: careful electronic evidence management processes and the use of

cryptanalysis, reidentification and digital forensics to uncover and preserve the chain of custody (Casey, 2019: 654; Dodge with Burruss 2020: 339). The technical complexity involved is often compounded by procedural difficulties in establishing cross-jurisdictional cooperation for the investigation of cybercrimes (Willits with Nowacki 2016: 120). There are significant impediments to successful cybercrime investigations. The Australia High-Tech Crime Centre (AHTCC) is an Australian-wide policing initiative to coordinate the efforts of law enforcement in Australia in combating serious, complex and multi-jurisdictional Internet-based crimes, particularly those beyond the capability of individual police agencies in Australia. Other roles include protecting the information and communications of Australia and providing information to other law enforcement to help combat online crime and to 'discover levels of online criminal activity and to undertake necessary measures to prevent or combat digital crime (Australia High-Tech Crime Centre, (2008).

The AHTCC establishes a guideline that quantifies and assesses which cybercrime is to be investigated first. The AHTCC assigns an investigative priority based on four different criteria: level of effect. The sophistication of the attack, the nature of the target, and the target significance (Australia High-Tech Crime Centre, 2008). The first criterion is the level of effect, which assesses the severity of the attack and damage inflicted on the victim which is either human or computer systems or networks. (Australia High-Tech Crime Centre, 2008). For example, online auction fraud, spamming and spreading viruses are excluded from the AHTCC priority of investigation (Australia High–Tech Crime Centre, 2008), because they do not inflict serious harm. Meanwhile, child cyber–pornography offences have received extreme attention, such as ' Operation Auxin' led by the Australia Federal Police (AFP) and 'Operation Cathedral' led by the National Crime Squad, a British police organisation, which was the world's largest policing operation against cyber paedophiles (Allyson & Spindles 2003:34). Sophistication of the attack, criterion number two, scale security breaches and discovers who is behind the attack, (Australia High-Tech Crime, 2008: 414). For example, attacks launched by organised crime or terrorist organisations receive a higher priority than hacking attacks. The third and fourth criteria assess the importance and the value of the victim.

3.10.5 The Electronic Crime Unit of South Africa Police

Cybercrime is prevalent in South Africa and external attacks are on the rise causing damage to companies and organizations (McNamara, 2012). The South Africa Electronic Crime Unit of the South Africa Police (SAP) is mandated to investigate all electronic crimes and conduct all digital forensic processes when cybercrime is reported. South Africa has enacted laws such as the Electronic and Cybersecurity Act (2020) that empower the electronic crime unit to conduct any form of investigation when crime has occurred. South Africa is rated among the countries showing the highest rates of cybercrimes in the world (Von Solms, 2015). The South African Police Services Directorate for Priority Crime Investigation (SAPS DPCI) also known as HAWKS highlighted that the occurrence of cybercrime in the country has gradually increased (Cole, 2013). The primary challenge facing South Africa is the lengthy development and implementation process of policies and mechanisms that combat cybercrimes. Because of high rates of evolution in cybercrime techniques and advancements in ICT, policymakers must be quick to shorten the gap between the development and efficient implementation of policy.

3.11. COMPARATIVE LEGAL ANALYSIS

Criminal investigations or crime investigations by investigators is a key proactive tactic that investigators or agencies mandated to investigate can employ to address virtual crime or cybercrime and other disorders by offenders. Mandated investigations agencies strive to find effective ways to determine whom they should target and how best to direct their resources. Virtual criminal investigations prioritisation by investigators is one of the best cost-effective methods for streamlining scarce resources and reducing crime. Investigations resources prioritizing is crucial in 21 century policing, where there are limited investigative budgets and increases on investigation agencies to be more efficient and evidence-based in their decision. Relative to other types of analyses, one could argue that crime investigators and their agencies have not been as rigorous or methodical about how they identify and prioritize their offenders (Bruce, 2014).

Recent law enforcement efforts to prevent crime have typically focused primarily on the place and high-risk offenders. Place-based crime prevention is supported by research findings including crime is not randomly distributed and that a small number of areas account for the majority of crime (Weisburd, 2015) and directing additional investigators resources to hot spot areas are known to show reductions in crime in these locations (Braga, Papachcritos, and Hureau, 2012) without appreciable displacement to surrounding areas (Bowers *et al*., 2011). The genesis of this comparativeness contributed by the countries under study indicated that there is no standardised method for prioritising crime investigations. For instance, the four criteria set by the Australia High-Tech Crime Center are reliable in yielding accurate information about the priority of crime investigation (Maghaireh, 2019: 96). Maghaireh, (2019: 96) posit that child online Pornography crime is on the high list of investigations for the Australia High-Tech Crime Centre since it has more negative effects on children within society. The United State application is more cumbersome because there is no mechanism to detect that the complaints are genuine and financial losses attributed to the crimes are accurate. In addition, commissioning a preliminary investigation is time-consuming and expensive because it involves technical and legal issues such as evidence collection, and cross-border laws since every state has its own (Maghaireh, 2019: 96). Ranking methodology or crime prioritization with high or low priority enhances law enforcement and investigators to determine their investigation on top offenders, and also for distribution of resources such as staffing and equipment for investigation of high–profile crimes. "In addition, it provides more consistency and clarity in the investigation process across the national and international levels (Maghaireh, 2019: 96). For example, on 01 March 2000, a computer hacker allegedly compromised multiple e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and stole as many as 28,000 credit card numbers with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites (FBI Cyber Division, 2000). After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) police service in a search at the residence of the subject who was then arrested in the UK along with a co-conspirator under the UK's computer misuse act of 1990." This case was predicated on the investigative work by the FBI, the Dyfed Powys

police service in the United Kingdom, Internet security consultants, the Royal Canadian Mounted Police (RCMP), and the international banking and credit card industry. This case illustrates the benefits of law enforcement and private industry, around the world, working together in partnership on computer crime investigations (FBI Cyber Division, 2000).

Also, crime investigation prioritisation helps cybercrime Units or investigators to make the links among investigation responsibilities and to assign the job to the right department. The general picture of the international level is that virtual criminal investigation prioritization varies widely. However, while developed countries like the United States, Australia, and United Kingdom display an extreme interest in pursuing, capturing and prosecuting paedophiles, Ghanaian Police Cybercrime Unit lack the technical skills which make the investigation approach of child online pornography crime nearly impossible. Given this, there is a need for a consensus investigation approach roadmap for Cybercrime Units from investigations agencies like the FBI, Europol, and Interpol and the M15 which will identify objectives, goals, resources, and investigation priorities among Cybercrime Units wide world of globally.

3.17 CHAPTER SUMMARY

Criminals are becoming more aware of digital forensic and investigation capabilities, and are making more sophisticated use of computers and networks to commit their crimes. Some are even developing “anti-forensic” methods and tools specifically designed to conceal their activities and destroy digital evidence, and generally undermine digital investigators. The integration of strong encryption into operating systems is also creating challenges for forensic examiners, potentially preventing us from recovering any digital evidence from a computer (Casey &Stellatos, 2008). Therefore, specialist toolkits are required for digital detective and investigation work. Digital detective investigators or computer forensic investigators must be equipped with the appropriate kits to collect, store, preserve, and transport forensic evidence since there is a growing trend toward relying on digital evidence, not only to prove straightforward charges, such as illegal possession of pirated software or child pornography but also to imply motive or intent by generating a digital profile of a crime suspect. Several computer forensic tools are

commercially available that can acquire both volatile and non-volatile data. The validity of some of these tools, such as Encase, and FTK has been upheld by the United States (U.S) court. Some experience is required to use these tools, and the type of tool that is ultimately used depends on the capabilities of the software and the operating systems of the computer or electronic device that will be examined for evidence.

CHAPTER FOUR

SEARCHING AND SEIZING DIGITAL EVIDENCE WITH AND WITHOUT WARRANT

4.1 INTRODUCTION

Technological advancement and the shift in crimes from brick and mortar to virtual environment targeted by faceless individuals has and will continue to have impact on

Ghanaian society and the global world. Considering the use of internet-based information systems in our everyday life, as well as the interconnectivity of multiples of computers through global networks has made virtual crime more dangerous and more globally important to combat than its brick and mortar counterparts. In this regard, criminal offences against computer technologies and its infrastructures assume various forms and have been labelled, inter alia, as virtual crime, computer crime, internet crime, information technology crime, high-tech crime, e-crime and cybercrime.

In the view of Basdeo *et al*., (2014:49) information technology crime does not require physical proximity between the victim and the perpetrator for the commission of the crime. Cybercriminals can virtually connect to information technology systems such as the internet from anywhere in the world Basdeo, *et al*., (2014:49). Meanwhile the criminal justice field lack behind and is not keeping pace with crime in the computing and electronic context. Today the policing of terrestrial space is very much a pluralistic pursuit. So too is the policing of cyberspace. Responsibilities for the control of cybercrime will be similarly shared between agents of the state, information security specialists in the private sector and individual users. Basdeo, *et al*., (2014:49)". reveal that the real-world limits of local, state and national sovereignty and jurisdiction cannot be ignored by law-enforcement officials. It can be a daunting task to obtain information from foreign countries, especially on an expedited basis – more specifically when the other country is in a different time zone, has different legal systems, does not have trained experts and uses different languages.

4.2 THE CONCEPT OF SEARCH IN DIGITAL CRIMINAL INVESTIGATION

Geberth (2015:217) posit that t he search of the crime scene is the most important phase of the investigation conducted at the scene. Ferdico, Fradella and Totten (2015:210) posit that search occurs when an expectation of privacy that society is prepared to considered reasonable is infringed. Decisions of the courts restricting the admissibility of testimonial evidence have significantly increased the value of electronic evidence in virtual criminal or cyber-criminal investigations. Ferdico *et al* (2009:210) further explain that seizure of property occurs when there is some meaningful interference with an individual's

possessory interests in that property. *United States v. Jacobsen, 446 U.S. 109, 113 (1984).* Therefore, law enforcement personnel involved in the crime scene search must arrange for the proper and effective collection of evidence at the scene.

Further explanation of search by Meeker (2005) is that it is a violation done by Government and quotes *Kyllo v. the United States,* 533 U.S.27 (2001) where the court proscribed the use of thermal imaging device without a warrant. The definition of "search" was protracted to encompass procuring information by sensing or enhancing technology regarding the interior of a home that could not contrarily have been retrieved without a physical intrusion into the home and search occurs when the anticipation of privacy that society regards reasonable is transgressed. A search is, therefore, viewed as constitutional if it does not infringe on a person's reasonable or legitimate apprehension of privacy. Electronic evidence, which is often referred to as the unimpeachable witness cannot be clouded by faulty memory, prejudice, poor eyesight, or a desire not to get involved. However, before a forensic laboratory can effectively examine electronic evidence, it must recognise it as evidence. Practically, anything and everything should be considered as evidence until proven differently. Once an item is recognised as evidence, it must be properly collected and preserved for laboratory examination. However, in order for electronic evidence or physical evidence to be admissible, it must have been legally obtained. The courts have severely restricted the right of the police to search certain crime scenes without a warrant.

For example, in *Mincey v. Arizona* 437 US 385(1978), the US Supreme Court said that the police had violated the defendant's Fourth Amendment rights. Mincey, who was a dope dealer had shot and killed an undercover narcotics officer during a drug raid. Mincey was wounded and one of his companions was killed in the subsequent gun battle. Following procedure, the narcotics officers secured the premises and notified Homicide. Homicide detectives conducted an investigation during which hundreds of pieces of evidence were seized by the police over a 3-day crime scene search (Gerberth, 2015:216). Mincey was convicted of the murder of the undercover officer. The conviction was overturned by the US Supreme Court, which maintained that Mincey's Fourth

Amendment rights were violated and that the police should have secured a search warrant (Gerberth, 2015:216).

Also, in 1999 the Supreme Court of USA once again stepped in to address the same issue raised in the Mincey v Arizona cases. This time it was in *Flippo v. West Virginia* 98 US 8770 (1999), Flippo was a pastor who reportedly was having a homesexual affair with a member of his congregation. His wife had discovered the relationship and was going to divorce him. Flippo convinced her that they should reconcile and talked her into going on a camping trip. They went to a cabin in West Virginia that the pastor had rented. While at the cabin, the pastor reported that they had become victims of home invasion during which his wife was fatally beaten and the pastor was slightly injured. The police were not impressed with Flippo's injuries. He was brought to a local hospital and "patched up" Investigators processing the crime scene came upon Flippo's briefcase. Inside the briefcase were various pornographic pictures of Flippo and his male lover engaged in sexual activities. These materials, which represented motive, is well as the other evidence seized from the cabin were introduced into trial, Flippo was convicted of the murder of his wife. The conviction was overturned based on the same issues raised in the Mincey and Arizona.

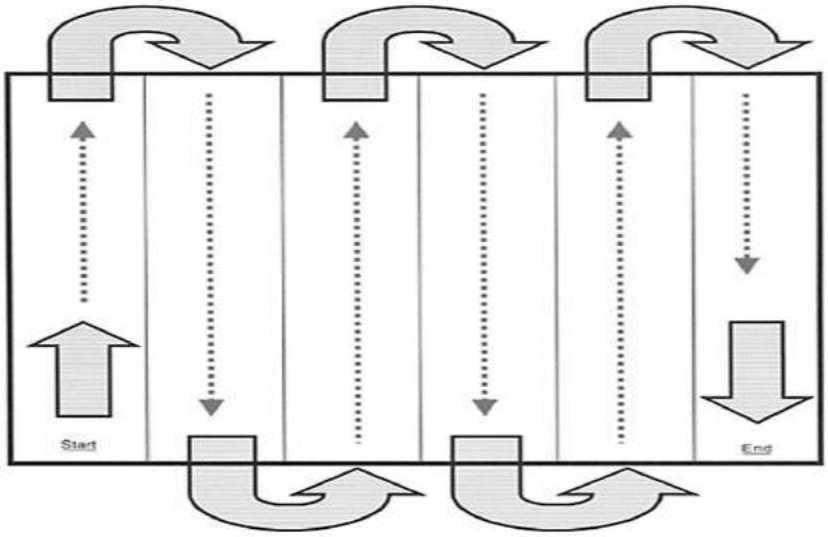
Sady (2012:4) argues that the definition of a search has significant exceptions contracted by an increasingly narrow view of anticipations of privacy deemed reasonable. For example, visual observations into the interior of a home may constitute a search or requiring a person to open a door so that the investigator has visual access to the interior of the house may constitute a search, even if there is no physical entry. According to Miller (2011), the preliminary crime scene search is usually done to establish physical evidence and orientate it before resorting to documentation. Miller (2011) illustrates as a safeguard to ensure no evidence is lost, that search methods have been developed and no single search method is relevant to specific types of scenes.

4.3 METHODS OF CRIME SCENE SEARCH

The method selected for the search of the crime scene is usually determined by the size location and complexity of the scene. Miller (2011) further stresses that the search methods used are geometric six patterns consisting of

4.3.1 The Strip Method

This method can be used effectively if the area to be covered is large and open. It is relatively quick and simple to implement and may even be performed by a single investigator in a limited area such as a room (Ross & Donna 2019:90). The strip search diagrammed in 4.1involves the demarcation of a series of lanes down which one or more person's proceeds. On reaching the starting point, the searchers proceed down their respective lane (Swanson *et a*l, 2019:80). On reaching the starting point, the searchers proceed down their respective lanes, reverse their direction at the end their lane, and repeat the process until the entire area has been covered. Whenever evidence is found, all searchers should be stopped and briefed about what was found to keep everyone informed (Swanson *et a*l, 2019:80). Figure 4.1 Depicts strip search method for crime scene investigation.

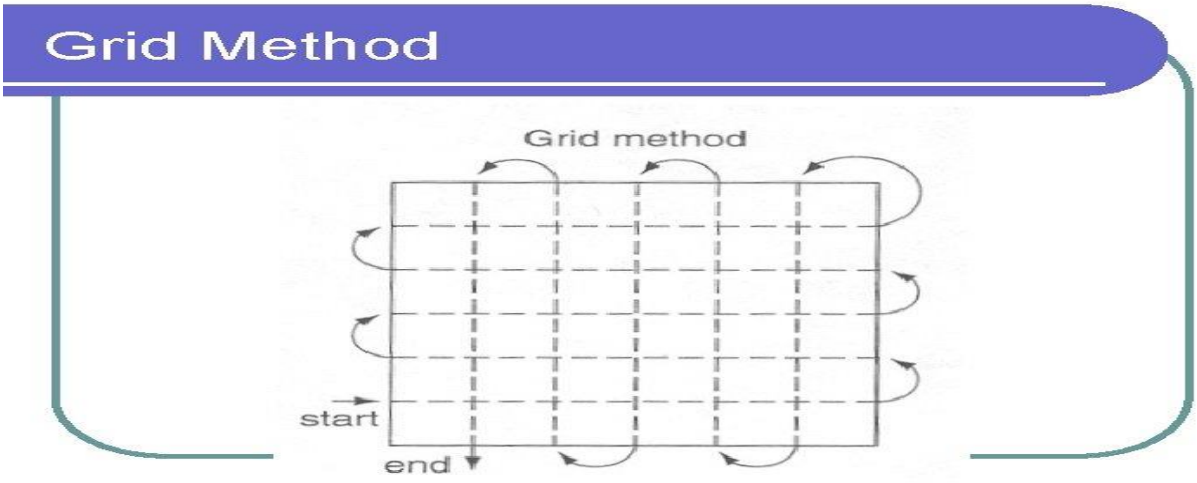


- Figure 4.1 Depicts diagram of strip search method for crime scene investigation. Source: Chegg

Ross and Donna (2019:90) also posit that, in the strip search, a searcher divides the area in question into a functional strip or lane. The searcher starts at one end of the scene and begins searching each strip, reversing direction at the end of a lane and searching the next adjacent strip until all areas have been evaluated (Ross & Donna, 2019:90).

4.3.2 The Grid Methods

Ross and Donna (2019:90) assert that the grid search is also a variation on the strip search. Instead of a single group of lanes, two groups are established at 90-degree angles to each other. Starting at one end, the searcher moves along the first group in the same fashion as a normal strip search. Swanson et al (2019:80) further emphasis that the grid search is a variation of the strip or line search pattern or method, and is depicted in Figure 4.2. Swanson et al (2019:80) state that after completing the strip pattern, the searcher double back perpendicularly across the area being examined. Although more time consuming than the strip search, the grid offers the advantage of being more methodical and through; examined from two different viewpoints, an area is more likely to yield evidence that might otherwise have been overlooked (Swanson et al, 2019:80)



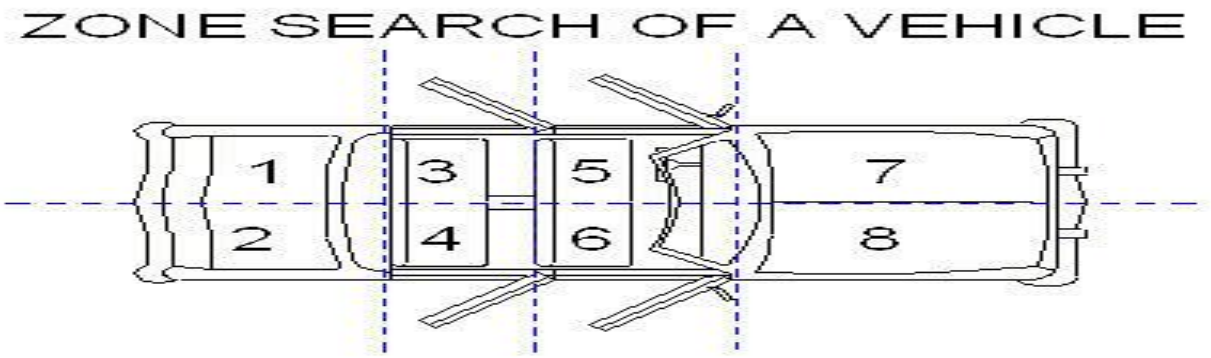
- Figure 4.2: Depicts diagram of grid search method for crime scene investigation. Source: Slideplayer. Source: Chegg

Ross and Donna (2019:90) further highlight that when the searcher reaches the end, s/he begins the second look over the same terrain, following the second set of lanes. This results in one searcher checking the area twice from two different perspectives.

4.3.3 The zone search

The area to be searched is divided into squares, sectors or variations. An officer is assigned to each zone or set of squares if the zones are further divided. This method is effective for indoor locations (Ross & Donna 2019:90). Figure 3.3 shows the zone search pattern which require that an area or the inner compartment of a car can be broken down into four areas or zones (Zone 3 to 6). The crime scene investigator checks each area thoroughly and independently of the other sections before moving on. This process will generally result in sufficient overlap to prevent items from being missed that may lie in between or under the seats near an adjoining zone. The hood and trunk are each considered an independent zone (Zone 1, 2, 7, and 8) and are dealt with accordingly. If the exterior of the car is under scrutiny for fingerprints, paint chips, bloodstains, or some other type of evidence, each side of the vehicle becomes a zone. The utility of the zone search is that it prevents the searcher from indiscriminately moving from one point of interest to another (Ross & Donna 2019:92). It forces the searcher to consider each area

independently and reduces the probability that an area

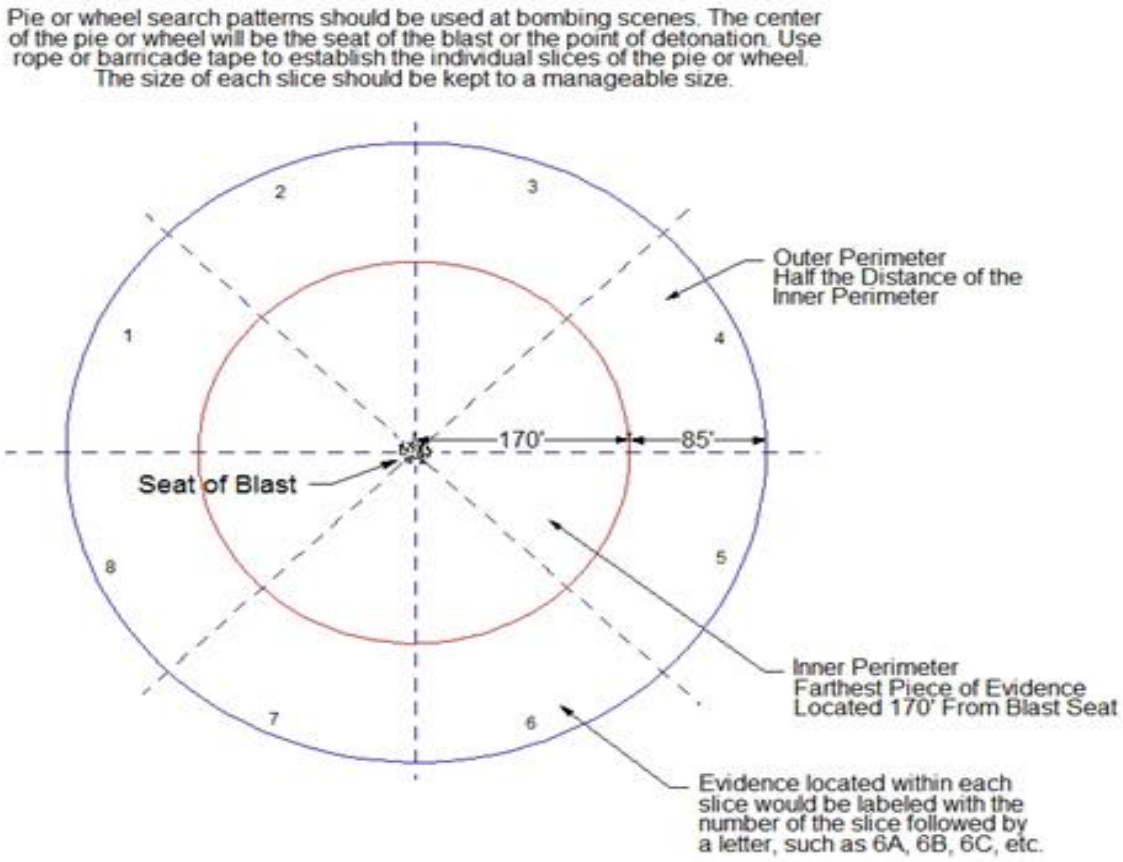


- Figure 4.3 Depicts diagram of zone search method for crime scene investigation.

will be overlooked .One variation of the zone search is to break down an area that is not easily checked with another patterned search into small, defined areas. The searcher checked each section independently before moving on to the next.

4.3.4 The wheel method

Swanson et al (2019:80) posit that the wheel search method entails dividing the area into a number of pie-shaped sections and is depicted in Figure 4.4. These are then searched, usually through a variation of the strip method. In practice, both the spiral and the pie search patterns are rarely employed (Swanson et al, 2019:80). The wheel search pattern or methods employ by several people moving from the boundary straight toward the Centre of the scene inward or from the Centre straight to the boundary outward (Saferstein, 2009:42). Geberth (2015:222) posit that in the wheel search pattern the searchers gather at the centre of the scene and move out in spoke-like directions. The obvious drawbacks of this method are the possibility of ruining evidence when gathering at the centre and the ever-increasing distance between searches as the investigators move outward (Geberth 2015:222).



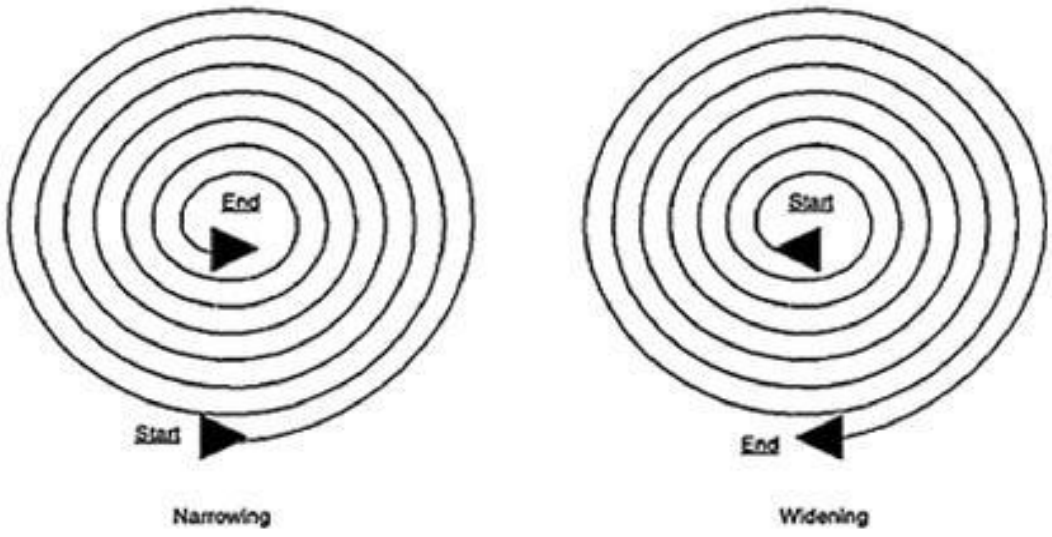
- Figure 4.4 Depicts diagram of wheel search method for crime scene investigation.

4.3.5 The Spiral method

The spiral search method is an effective method that is widely employed in interior scenes (Ross & Donna 2019:92). The searcher begins on the outside of the area or room and then, moving in a slow circle, search in a spiral pattern inward, as seen in figure 4.5. The width of the swath or area being evaluated with each spiral is scene-dependent. The circle search is also employed in reverse, by moving outward from a primary focal point or the centre of a room. The only critical consideration in the circle search is managing the pace of the search. As the circle closes, the searcher often begins moving along the path of the spiral at a faster pace. The searcher must consciously slow his or her speed as the

area remaining to be examined narrows. Whether moving inward or outward, the searcher must maintain a pace that allows a full evaluation of the area in question (Ross &

Donna 2019:92).



- Figure 4.5 Depicts diagram of spiral search method for crime scene investigation. In the spiral search or circle search, the searcher moves through the scene using a spiralling pattern. Source: Chegg

4.3.6 The line method

Geberth (2015:222) state that the line method is used for outdoor scenes and can be difficult to search due to vegetation and topography. One of the quickest and easiest methods to utilise is the line search (Geberth, 2015:222). The officers are lined up next to one another and proceed along a straight line as they search a designated area. In the line search, a large group of searchers line up on the lanes and move down the strips together in a single direction, each evaluating their particular lane, as seen in figure 6. The number of searchers necessary is, of course, scene-dependent (Geberth, 2015:222). This method is particularly useful in dealing with the exterior scene over uneven terrain. The most critical consideration for the search team is to move the group together as a

single entity. Searchers should remain online, moving at the pace set by the slowest searcher.

- Figure 4.6: Depicts diagram of line search method for crime scene investigation. Source: quizlet.

The line search is a variation on the strip search. It is effective when dealing with uneven terrain (Ross & Donna 2019:92). A group of searchers is lined up along the lanes and moves in a single direction from a start line to an end line. Each searcher is responsible for evaluating a single lane Ross & Donna 2019:92). To keep the line moving, as items are encountered, the evidence is flagged, and a team comes in behind the searchers to process the evidence.

4.4 DEFINING THE TERM "SEARCH WARRANT"

Marras (2015) states that search warrants provide law enforcement agencies with the authority to enter premises, search for the objects named in the warrant, and seize them. To be valid, the warrant must specifically state the crime being investigated, the location to be searched, and the items to be seized (Marras, 2015). The definition of a search

warrant helps explain the scope and boundaries of investigation procedures. Therefore, the doors are open for legal scholars and judges to define a search warrant. Gino (2003:222) purports that a search is a written document that represents judicial authorisation for peace officers to enter and search a specific place for specific items and to seize those items that are evidence of the offence if they are found. In addition, Freedman (1999:8) asserts that a search warrant is an order signed by a judge or a magistrate that authorises police officers to search for specific objects or materials at a clearly defined location at a specific time.

Ferdico, *et al* (2015:212) agrees that a search warrant is an order in writing, issued by a proper judicial authority, in the name of the people, directed to a law enforcement officer, commanding the officer to search for certain personal property and commanding the officer to bring that property before the judicial authority named in the warrant. Law enforcement officers applying for search warrants must follow established laws and procedures. Otherwise, a magistrate will deny the application or a court will invalidate an illegally issued warrant. In either instance, valuable evidence may be lost to the prosecution. Search warrant procedures are set out in statutes, rules, and court decisions that vary among different jurisdictions.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

) Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ❒ evidence of a crime;
- ❒ contraband, fruits of crime, or other items illegally possessed;
- ❒ property designed for use, intended for use, or used in committing a crime;
- ❒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*

The application is based on these facts:

- ❒ Continued on the attached sheet.
- ❒ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

_____
Applicant's signature

_____
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

_____
Judge's signature

City and state: _____

_____
Printed name and title

- Figure 4.7 Shows an example of a Typical Search Warrant. Source: US Department of Justice

4.4.1 Contents of the Search Warrant

According to Ferdico *et al* (2015:230), search warrants vary among jurisdictions or countries, most search warrants contain the following information:

(a) The caption of the court or division of the court from which the warrant is issued.
(b) A particular description of the place or person to be searched.
(c) A particular description of the property to be seized.
(d) A statement of grounds for issuance of the warrant.
(e) The names of persons whose affidavits have been taken in support of the warrant.
(f) The names of the officer or class of officers to whom the warrant is directed together with a command to search the person or place named for the property specified.
(g) A specification of the time during the day when the search may be conducted
(h) The date of issuance.
(i) The signature of the issuing magistrate together with a statement of the magistrate's official title.

4.4.2 Who May Issue Search Warrant

Only judicial officers who have been specifically authorised to do so may issue search warrants. Most jurisdictions give this authority to judicial officers such as clerks of court, magistrates, complaint justices, justices of the peace, and judges. Law enforcement officers need to know which judicial officers are authorized to issue search warrants in their jurisdictions. They may be from the judicial officers authorised to issue arrest warrants. A search warrant issued by a person without authority has no legal effect, and

a search made under such a warrant is illegal. In *Shadwick v. City of Tampa*, 407 U.S. 345 (1972), the U.S. Supreme Court rejected the notion that all warrant authority must reside exclusively in a lawyer or judge and upheld a city charter provision authorizing municipal court clerks to issue arrest warrants for municipal ordinance violations. The Court held that "an issuing magistrate must meet two tests. He must be neutral and detached, and he must be capable of determining whether probable cause exists for the requested arrest or search (*Shadwick v. City of Tampa*, 407 U.S. 345 (1972)."

4.4.3 Probable Cause for Issuance of Warrant

According to Swason, *et al* (2019:625), the general requirements for searches and seizures of evidence or persons are a search warrant or recognized exception to the warrant requirement and probable course. Marras (2015:88) posits that search warrants must be supported by probable cause, and objects of the search must be described with sufficient particularity. Ferdico, Fradella, Totten (2012:212) agrees that, before issuing a search warrant, the magistrate must have probable cause to believe that items subject to seizure are in a particular place or on a particular person at the time the warrant is issued. Law enforcement officers applying for a search warrant must supply the magistrate with the grounds for issuance of the warrant (Ferdico *et al,* 2015:212). Probable cause exists where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found (*Ornelas v the United States 517 U.S. 690, 696 [1996]).* Marras (2015:88) argued that when applying for a search warrant, an investigator must demonstrate probable cause both that a crime has been committed and that the evidence of the crime will be found in the location specified in the warrant. Consider the crime of sending or receiving child pornography. Some courts have held that an individual's membership in a child pornography site shows the probable cause of the receipt or distribution of child pornography (*United States v. Martin,* 426 F. 3d 3 2d Cir. [2005]); (*the United States v. Wagers,* 339 F Supp. 2d 934 [2004]).

In the matter of *United States v. Bailey,* 272 F.Supp. 2d 822 (2003), the court stated that when an individual knowingly becomes a computer subscriber to a specialized internet

site that frequently, obviously unquestionably, and sometimes automatically distributes electronic images of child pornography to other computer subscribers, [that action] alone establishes probable cause for a search of the target subscriber's computer even though it is conceivable that the person subscribing to the child pornography site did so for innocent purposes and even though there is no direct evidence that the target subscriber received child pornography on his or her computer.

Also, probable cause to search and seize exists when facts and circumstances in a given situation are sufficient to warrant a person of reasonable caution to believe that sizeable objects are located at the place to be searched. The facts and circumstances that would justify an arrest may be different from those that would justify a search. The definition of probable cause in *Illinois v. Gates,* (462 U.S. 213, 1983), is helpful in this regard and is state that: “Probable cause according to its usual acceptation means less than evidence which would justify condemnation….." Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision. While an effort to fix some general, numerically precise degree of certainty corresponding to "probable cause" may not be helpful, it is clear that "only the probability, and not a prima facie showing, of criminal activity, is the standard of probable cause." The gates opinion also said that the central teaching of our decisions bearing on the probable cause standard is that it is a practical, non-technical conception. "In dealing with probable cause….as the very name implies we with probabilities. These are not technical, they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act" said the court *Illinois v. Gates* 462 U.S.at 231 [1983]. Stated simply, probable cause to search is “a fair probability that contraband or evidence of a crime will be found in a particular place” *Illinois v. Gates,* (462 U.S.231 [1983]). And probable cause to arrest is a fair probability that a particular person has committed or is committing a crime.

Some jurisdictions require that an affidavit contain all the information on which a magistrate is to base a finding of probable cause to issue a search warrant (*Valdez v. State*, 476 A. 2d 1162 Md.[1984]). Other jurisdictions allow supplementation of a defective

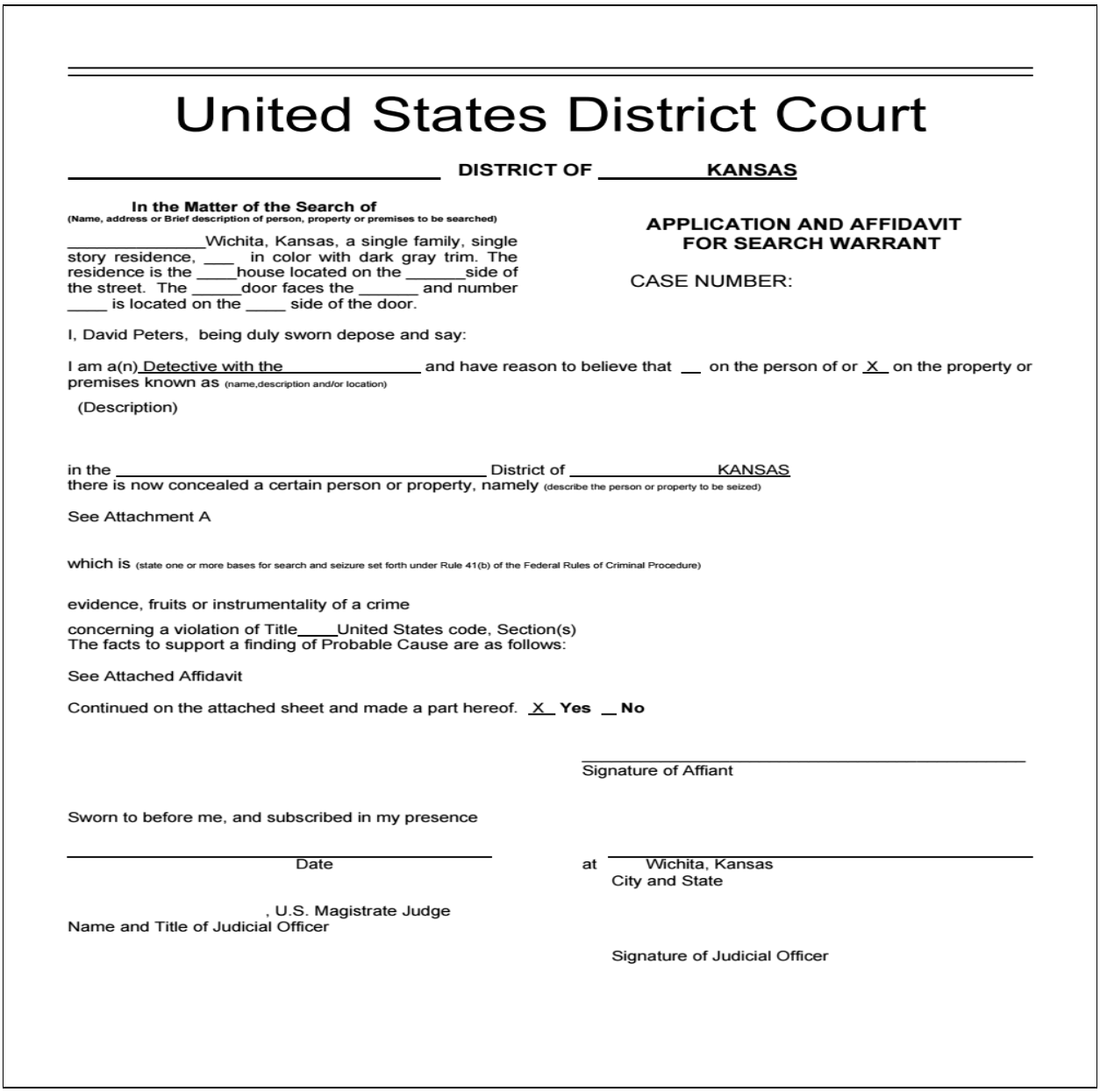
or incomplete affidavit by sworn oral testimony given before the magistrate (*state v. Hendricks*, (328 N.E. 2d 822 Ohio [2015]).

Several jurisdictions permit the issuance of search warrants over the telephone or by e-mail or facsimile (FAX), but still, require that the information provided by the affiant to the magistrate be taken under oath and recorded (Ferdico 2012:210). All the information on which probable cause is based should be written in the affidavit. This forces law enforcement officers or the cyber-criminal investigator to think carefully about cases before applying for a warrant, and provides a complete record for reviewing courts to evaluate the magistrate's decision if the warrant is challenged. Therefore, the affidavit is the exclusive vehicle for applying to a magistrate for the search warrant. An affidavit for a search warrant should inform a magistrate that a criminal offence or cyber-criminal offence has been or is being committed and that seizable evidence relating to that offence is in a particular place at a particular time. The affidavit must state the underlying facts and circumstances on which probable cause is based. The totality of the facts and circumstances must show "a fair probability that contraband or evidence of a crime will be found in a particular place" (*Illinois v. Gates*, 462 U.S. 213, 238 [1983]).

Time is a very important factor in determining probable cause to search. If the information on which probable cause was initially based becomes stale, there may no longer be a good reason to believe that property is still at the same. In *United States v. Wagner,* (989 F2d 69 2d Cir.), the information supporting probable cause to search the suspect's home was (1) a single small purchase of marijuana from the suspect in her home more than six weeks be the search, (2) a recorded statement of the suspect identifying her source for the marijuana, and (3) an unsubstantiated assertion that the suspect's home was owned by the source.

These facts were insufficient for the court to find that the suspect engaged in continuing criminal activity in her home as a member of the source's drug distribution network. Because marijuana is the type of property that is likely to disappear or be moved, probable cause was found to be stale at the time the warrant was issued and the search was conducted. The length of time that an item of property is likely to remain at a given location

depends on the nature of the property, the nature of the criminal activity, the duration of the criminal activity, the criminal suspects, and many other factors.



United States District Court

_____ **DISTRICT OF** _____**KANSAS**

In the Matter of the Search of
(Name, address or Brief description of person, property or premises to be searched)

_____Wichita, Kansas, a single family, single story residence, ____ in color with dark gray trim. The residence is the _____house located on the _____side of the street. The _____door faces the _____ and number _____ is located on the _____ side of the door.

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER:

I, David Peters, being duly sworn depose and say:

I am a(n) Detective with the _____ and have reason to believe that __ on the person of or X on the property or premises known as (name,description and/or location)

(Description)

in the _____ District of _____KANSAS
there is now concealed a certain person or property, namely (describe the person or property to be seized)

See Attachment A

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence, fruits or instrumentality of a crime

concerning a violation of Title____United States code, Section(s)
The facts to support a finding of Probable Cause are as follows:

See Attached Affidavit

Continued on the attached sheet and made a part hereof. X **Yes** __ **No**

_____
Signature of Affiant

Sworn to before me, and subscribed in my presence

_____ at _____
Date Wichita, Kansas
City and State

, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

- Figure 4.8 Show an example of a Typical Affidavit for a Search Warrant. Source: US District Court Wichita Kansas.

In *United States v. Laury,* 985 F.2d 1293 5th (Cir.1993), the court found probable cause to search a suspected bank robber's home for instrumentalities and evidence of the crime was not stale, even though nearly two months had passed since the date of the robbery. The affiant, an expert in bank robbery investigations, stated that bank robbers tend to keep evidence of the crime in their home for as long as several years. In virtual crime, internet crime or cybercrime the investigator must establish reasonable grounds or probable cause to believe that a person has committed or is committing a crime is quite different from establishing grounds for conventional searches. In traditional searches or conventional searches, the investigator or police find no problem in establishing a connection between facts, materials or items stated in the warrant and the physical location or place to be searched. For example, if reliable rape or sexual assault crime information is received by the police or investigator and there is an indication that crime is being committed, or has been committed, the police or investigator will be able to prepare an affidavit stating the items to be searched and the crime location on the basis of which the magistrate will grant the warrant. In other instances, the role of the computer determines any alleged crime and also shows particularised facts demonstrating how materials of evidence which are impalpable are linked to the crime's physical location if the police officers or investigators receive reliable information concerning cybercrime.

There are significant roles played by ISP in providing information to officers establishing connections between the items stated or described in the warrant and the physical location to be searched. For instance, when an offender commits Denial of Service (DoS) attack crime, investigators will contact the Internet Service Provider of the offender to obtain information concerning the IP address that identifies the offender or the attacker's connection. When the IP address is issued to the police or investigator an examination will be conducted to assist the law enforcement officer or the investigator to have sufficient proof to establish a probable cause basis for the issuance of the warrant. However, the nature of cyberspace which knows no physical boundaries cripples the investigator's

ability to easily establish a factual nexus between the items described in the warrant and the physical location or place to be searched.

The Internet Protocol address plays a critical role in locating the physical address of the suspects in a wide range of cybercrimes and can identify a person who allegedly posted personal details and sexually suggestive comments. One relevant case in this regard is *United State v. Hamilton*. In this case, Kenneth Hamilton was suspected of downloading child pornography and distributing it on the Internet. Law enforcement officers investigating this incident found a link between Hamilton and the child pornography pictures. Specifically, the computer-generated header information attached to the child pornography pictures revealed the screen name of the person who posted them, the date each images was posted, and the Internet Protocol (IP) address of the individual who posted them (Marras 2015:42). However, the role varies between dynamic and static IP addresses both of which are automatically assigned by Internet Service Providers (ISPs) to their subscribers. A dynamic IP address is assigned to subscribers using a Dial-Up connection for Internet access and an Internet Protocol (IP) address offers the users anonymity by providing a temporary Internet Protocol address to the user's device each time it connects to the internet. When a user disconnects from the Internet the Internet protocol address is terminated and will be assigned to a new user when. In several instances, capturing suspect Internet Protocol addresses and his physical location is impossible because of the short lifetime and mobility of the dynamic Internet Protocol addresses, but a static IP address is assigned a unique number permanently assigned to a computer device connected to the Internet located in a fixed place.

4.5 THE SEARCH WARRANTS

4.5.1 The Scope of Search Warrants

A search warrant authorizing the search of particularly describe premises justifies a search of the described land, all of the buildings on the land, and other things attached to or annexed to the land (*United States v. Meyer,* 417 F:2d 1020 [8th Cir. 1969]). Courts

also generally allow a search of any vehicles owned or controlled by the owner of the premises and found on the premises (*United States v. Percival,* 756 F.2d 600 [7th Cir. 1985]). Carmen (2013:255) indicates that the scope and manner of the search must be reasonable based on the object of the search. According to Ferdico (2013:315), a search of areas neighbouring or adjacent to the particularly described premises is usually not allowed. Carmen (2013:235) states this example, suppose a search warrant is issued for the recovery of a stolen 25-inch Zenith TV set. In looking for the TV set, the officer cannot open lockers and drawers—unless, of course, the locker or drawer is big enough to contain the TV set. But, if the search warrant is for the confiscation of heroin, then the officer is justified in opening lockers and drawers in the course of the search. It, therefore, follows that the smaller the item sought, the more extensive the scope of allowable search. If neighbouring or adjacent areas are only nominally separate, however, and are actually used as a single living or commercial area, courts may allow the search of the entire area despite a limited warrant description (Ferdico *et al* 2015:314). While the search is being conducted, the police may detain persons who are on the premises to search them (*Michigan v. Summers,* 452 U.S. 692. [1981]). However, these people must have been named in the warrant. For example, a search warrant for a bar and the bartender does not authorize body searches of all bar patrons (*Ybarra v. Illinois,* 444 U.S. 85 [1979]). Also, In *United States v. Elliott,* 893 F2d 220 (1990) held that the search of a storeroom behind an apartment did not exceed the scope of the warrant authorizing the search of the apartment. The storeroom was accessible through a hole cut in the wall of the suspect's bathroom and was covered by a burlap bag. The court found that the unconventional means of access did not sever the room from the rest of the apartment. In *United States v. Principe* 499 F.2d 1135 (1974), a search of a cabinet in a rant was justified when the owner testified that the cabinet "went with the apartment.

Officers executing a search warrant may look only where the items described in the warrant might be concealed. The court in *United States v. Ross,* 456 U.S. 798 (1982) stated the general rule: "A law fixed premises generally extends to the entire area in which the object of the search may be found and is not limited by the possibility that separate acts of entry or opening may be required to complete the search."

The court provided examples of the application of the rule: (a) warrant that authorizes an officer to search a home for illegal weapons and also provides authority to open closets, chests, drawers, and containers in which the weapon might be found. (b) a warrant to open a footlocker to search for marijuana would also authorise the opening of packages found inside. (c) a warrant to search a vehicle would support a search of every part of the vehicle that might contain the object of the search. In *State of Arizona v. Dean* 203 Ariz. 408. (2002) the Arizona Court of Appeals held that, based on an allegation of child sexual abuse, police officers obtained a search warrant for Thomas Dean's trailer and car. While searching the trailer, officers seized a laptop, later discovered to contain child pornography. Dean filed a motion to suppress evidence from the search on the grounds that the warrant lacked "particularity in describing the places to be searched and the items to be seized." Despite finding the warrant deficient of probable cause for possession of child pornography, the trial court found that the good faith exception to the warrant requirement applied. Dean appealed the trial court's denial of his motion to suppress, claiming that the fourth exception applied. When a legitimate search is underway, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand.

In *Wyoming v. Houghton* 526 U.S. 295, (1999), the court extended the permissible scope of the search of an automobile, holding that "police officers with probable cause to search a car may inspect passengers belongings found in the car that are capable of concealing the object of the search." An inaccurate description of the premises to be searched may cause officers to exceed the scope of a warrant, especially with respect to multiple-occupancy dwellings. In *Maryland v.Garrison* 480 U.S. 79 (1987), officers obtained and executed a warrant to search the person of Lawrence McWebb and the premises known as 2036 Park Avenue third floor apartment. The officers reasonably believed, on the basis of the information available, that only one apartment was located on the third floor. In fact, the third floor was divided into two apartments, one occupied by McWebb and one by the defendant. Before the officers discovered that they were in the wrong person's apartment, they had discovered contraband that led to the defendant's conviction. The court held that

the officers had made a reasonable effort to ascertain and identify the place intended to be searched and that their failure to realize the overbreadth of the warrant was objectively understandable and reasonable. Therefore, although some latitude is allowed for an honest mistake in executing search warrants, officers may not rely blindly on the descriptions in a warrant but must make a reasonable effort to determine that the place they are searching is the place intended to be searched.

In cyber search scope, the most important decision for an investigator during an application and affidavit for search describe the property in the warrant whether it is hardware or software. Computer hardware and software are the two vital components. Hardware components consist of the physical devices around the computer systems such as a keyboard, mouse, motherboard, visual display unit (VDU), and printers. Storage media such as floppy disks, hard disks, zip disks, jazz disks, cartridges, magnetic tape, magnet and optical cartridges, CD-ROM, CD-R, CD-RW and DVD. The software components consist of the programmes and data. Law enforcement should describe in the warrant if the computer hardware is contraband, evidence, fruits, or instrumentalities of crime, the warrant should describe the hardware itself and if the probable cause relates only to information. However, the warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored.

Seizing of hardware depends on the nature of the crime being committed by the offender and the kind of investigation conducted by law enforcement. Computer Hardware can be contraband, an instrumentality of a crime, or fruits of crime and therefore may be physically seized. For example, law enforcement can be compelled through a warrant to seize a computer that stores child pornography *United States v. Hay* 231 F.3d 630, 637 (9th Cir. 2000),, A computer may also be used as an instrumentality of crime, as when it is used to commit a hacking offence or send threats (*United States v. Adjani),*

4.5.2 Subject of the Search Warrant

In general, the items to be searched and seized must be described with sufficient particularity so that the officer executing the warrant can identify the items with reasonable

certainty and also is left with no discretion as to which property is to be taken. Ferdico (2012:221) highlights that the primary concern of courts evaluating descriptions of things to be seized in search warrants is to ensure that a person will not be deprived of lawfully possessed property by a seizure made under an imprecise warrant. A description of items merely as stolen goods, obscene materials, or another article of merchandise too numerous to mention is inadequate because it is imprecise. For example, *Marcus v. Search Warrant*, (367 U.S. 717 [1961]), full title *Marcus v. Search Warrant of Property at 104 East Tenth Street, Kansas City, Missouri*, is an *in rem* case decided by the US Supreme court on the seizure of obscene materials. The Court unanimously overturned a Missouri Supreme Court decision upholding the forfeiture of hundreds of magazines confiscated from a Kansas City Wholesaler. It held that both Missouri's procedures for the seizure of allegedly obscene material and the execution of the warrant itself violated the Fourth and Fourteenth amendments' prohibitions on search and seizure without due process. Those violations, in turn, threatened the rights protected by the Firth Amendment (*Marcus v. Search Warrant*, 367 U.S. 717 [1961]). In the cyber world, when data is contraband, evidence, or instrumentalities of crime, the subject of the search will be intangible items, such as data, images, files, and so on. Traditionally, search warrants have been used to search and seize tangible things, being the fruit of the crime, the object of the crime, or the instrumentality of the crime, such as illegal drugs, stolen property, cash, and weapon. The officers enter the nominated premises, search evidence by entering the room, opening drawers and looking around and then seizing tangible objects.

Maghaired (2012:121) states that investigators enter a real home or other building and search and seize data or they seize hardware, such as disks, and then make a mirror copy. In addition, Kerr (2013:109) states that the investigator acquires evidence by entering digital commands through a keyboard or using the forensic tool to retrieve the requested contents from the mirror copy and sending it to an output device, such as a monitor, printer, or peripheral to display the evidence. The affidavit supporting a request for a search warrant must contain a particular description of the items to be seized. When an item can be described in detail, all available information about it should be included in the affidavit. For example, number, size, colour, weight, condition, brand name, and other distinguishing features of an item to be seized also indicate how the item is connected

with criminal activity by stating the category of items subject to seizure within which the item falls. In *Re Grand Jury Investigation Concerning Solid State Devices, Inc. v. United States 130 F.3d 853 (1997),* Solid State Devices, Inc. and Unisem International (collectively "SSDI") appeal the district court's decision to deny their petition for return of the property, filed pursuant to Federal Rule of Criminal Procedure 41(e). SSDI's property was seized in connection with a Department of Defense ("DoD") investigation of alleged fraudulent practices. SSDI challenges the legality of the seizure, arguing that the warrants executed against it were insufficiently specific. We have jurisdiction pursuant to 28 U.S.C. § 1291, and we reverse the district court's denial of SSDI's Rule 41(e) motion.

4.5.3 Searching and Seizing Hardware and Software as Evidence

Many investigations seek to search computers for evidence of a crime only. The computer might contain business records relevant to a white-collar prosecution, for example, but the computer itself does not store contraband and was not used to commit the crime. When electronic storage media are to be searched because they store information that is evidence of a crime, the items to be seized under the warrant should usually focus on the content of the relevant files rather than the physical storage media. Computer hardware might itself be contraband, an instrumentality of a crime, or fruits of crime and therefore may be physically seized For example; a computer that stores child pornography is itself contraband. In the *United States v. Hay* 231 F.3d 630, 637 (2000), after Hay was indicted for possessing and distributing child pornography, he moved to suppress this evidence for lack of probable cause to search and on the ground of staleness, but the district court denied the motion. The district court also denied Hay's motion. to reconsider and to hold an evidentiary hearing in order to challenge the veracity of Galante's affidavit under Franks v. Delaware, 438 U.S. 154 [1978]). Hay never challenged the indictment or the instructions on this ground. Indeed, he stipulated that the computer graphics files recovered from his system involved children under the age of eighteen and the stipulation listed the age range of each child in each of the exhibits. Counsel conceded that the material was child pornography. Even assuming the issue is not waived, only one of the counts was charged under S 2256(8) and it does not focus on the two phrases at issue in Free Speech.

A computer may also be used as an instrumentality of crime, as when it is used to commit a hacking offence or send threats or a computer used to operate a bulletin board distributing obscene materials is instrumentality. In *Davis v. Gracey*, 111 F.3d 1472, 1480 (1997), the court held that the officer's reliance on a valid warrant entitled them to qualified immunity on plaintiffs' Fourth Amendment claim, and established a good faith defence under the Electronic Communication Privacy Act. The court also conceded that it lacks "subject matter jurisdiction over plaintiffs' asserted claim against the officers under the Privacy Protection Act and the court affirms the district court's entry of summary judgment for the officers."

The computer is "evidence" only to the extent that some of the data it stores is evidence. In *United States v. Giberson,* 527 F.3d 882, 887 (2008), Giberson appealed from the district court's denial of his motion to suppress evidence of child pornography found on his personal computer, which led to his conviction for receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and possession of child pornography in violation of 18 U.S.C.§ 2252(a)(4)(B). He also appeals his sentence, arguing the district court erred in sentencing him for both possession and receipt of child pornography. But the court held that they have jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a)(1) and therefore affirm his conviction, vacate his sentence, and remand. When probable cause to search relates in whole or in part to the information stored on the computer, rather than to the computer itself, the warrant should identify that information with particularity, focusing on the content of the relevant files rather than on the storage devices which may happen to contain them. In *United States v. Otero* 563 F.3d 1127 1132 (10th Cir. 2009), the court held that the district court agreed and suppressed the evidence. The government filed this interlocutory appeal under 18 U.S.C. § 3731. While the judges agree with the district court that the warrant was invalid for lack of particularity, the judges hold that the good faith exception to the exclusionary rule should apply and, accordingly.

Law enforcement should be particularly careful when seeking authority to seize a broad class of information. This sometimes occurs when agents plan to search computers at a business as observed by the court in *United States v. Leary,* 846 F.2d 592, 600-04 (10th

Cir. 1988). It held that the government appeals from the district court's decision granting the defendant's motion to suppress evidence seized under a search warrant. judges affirm the district court, holding that the defendant's fourth amendment rights were infringed, that the search warrant was facially overbroad and invalid, and that the evidence seized should be suppressed. Agents cannot simply request permission to seize “all records” from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business *(United States v. Ford,* 184 F.3d 566, 576 (6th Cir. 1999), Instead, the description of the files to be seized should be limited. One victorious method has been to point out records that show or make a connection to a particular crime and to include specific categories of the types of records likely to be found. For example, the Ninth Circuit upheld such a warrant that limited the search for evidence of a specific and specified crime (*United States v. Adjani,* 452 U.S.1140, (2006). It is sometimes helpful to also specify the target of the investigation (if known) and the time frame of the records involved if known (*United States v. Kow,* 58 F.3d 423, 427 9th Cir. (1995).

4.5.4 Multiple Affidavits

Ferdico (2012:212) assert that a law enforcement officer applying for a search warrant may submit more than one affidavit to the magistrate. The officer or someone else may prepare the additional or supplemental affidavit. The essential requirement is that all affidavits are satisfactorily incorporated into all related documents necessary to the application for the warrant. Ferdico *et al* (2015:226) outlines the following procedure for multiple affidavits to ensure proper incorporation:

(i) Entitle the first or primary affidavit “ Affidavit and Request for search Warrant”
(ii) Entitle all additional affidavits “Supplemental Affidavit 1,” “Supplemental Affidavit 2,” and so forth.
(iii) Include the following statement in the first or primary affidavit: “This request is also based on the information in the sworn statements in

Supplemental Affidavit 1, Supplemental Affidavit 2, Which are attached."

(iv) Securely attach all supplemental affidavits to the primary affidavit. Use a stapler or other semi-permanent method of binding. A paper clip is unsatisfactory because of its tendency to slip off.

By following these simple steps, the officer ensures that the magistrate will be simultaneously presented with all the information on which probable cause is to be based and that the appellate court will be able to effectively review the magistrate's decision (Ferdico *et al* 2015:222). In the case of *State v. Gamage*, 340 A. 2d 1,7 (1975), the court held that since the object of the processing before the magistrate is to establish probable cause to justify the issuance of a search warrant, law enforcement officers should not be hindered in their efforts to describe the basis for probable cause in supporting affidavits. So long as these affidavits are satisfactorily incorporated to all related document necessary to the application for the warrant… the reviewing court will be assured of the simultaneous presence of these documents before the magistrate, and the search may be subjected to authoritative judicial review.

4.5.5 Anticipatory Search Warrants

Over the years, a substantial number of people have heard a knock on the door accompanied by the ominous announcement of police authority to enter and search. A small but recently growing number of those searches have been conducted under the authority of anticipatory search warrants. Adams (2016:79) posit that an anticipatory Search warrant also called a prospective search warrant, is a warrant to search a particular place for a particular sizeable item that has not yet arrived at that place. Law enforcement officers are increasingly applying for anticipatory search warrants, especially in cases involving contraband in the mail and informants or undercover officers. An anticipatory search warrant generally is a warrant conditioning a search on an event that is to occur after the issuance of the warrant. In addition, an anticipatory search warrant is a warrant obtained based on probable cause and on an expectation that sizeable items will be found at a certain place at a certain time.

In a matter of *United States v. Grubbs, 547 U.S.* (2006), the Court decided that "anticipatory" search warrants are valid. In this case, a judge issued an anticipatory search warrant for the suspect Grubb's house based on a federal officer's affidavit, which explained that the warrant would not be executed until a parcel containing a videotape of child pornography which Grubbs had ordered from an undercover postal inspector was received at, and physically taken into, the residence. Grubbs was seized by the officers after the package was delivered. During his trial for receiving child pornography, Grubbs moved to suppress the evidence. On appeal, the Court rejected his arguments and said that "anticipatory warrants are not categorically unconstitutional under the Fourth Amendment's provision" as long as there is probable cause. The Court added that "when an anticipatory warrant is issued, the fact that the contraband is not present at the place described is immaterial, so long as there is probable cause to believe it will be there when the warrant is executed." A judge or magistrate is not required to issue an anticipatory warrant, so it is a matter of judicial discretion. But if the judge or magistrate decides to issue it, the warrant is valid (Carmen 2013:217).

Although anticipatory search warrants are not constitutionally forbidden, a warrant conditioned on a future event presents a potential for abuse above and beyond that of a traditional warrant. Officers executing anticipatory warrants must determine when and whether the triggering event specified in the warrant occurs. Therefore, magistrates issuing anticipatory warrants must be particularly vigilant to ensure that opportunities for exercising unfettered discretion are eliminated. To satisfy these concerns, the magistrate must set conditions governing the execution of an anticipatory warrant that are explicit, clear and narrowly drawn so as to avoid misunderstanding or manipulation by government agents. In *state v. Vitale,* 530 P2d 394 (1975), the court invalidated an anticipatory search warrant for failure to satisfy the "sure and irreversible course" requirement. In that case, a warrant to search the defendant's pawnshop was issued on the basis that a reliable informant had agreed to sell a stolen television set to the defendant at the pawnshop. The police had the television in their possession at the time they applied for the warrant. After the sale, the warrant was executed and the television was seized. The court held that there was no probable cause that a crime had been committed at the time the warrant was issued. To ensure that a magistrate is provided with sufficient information to justify

the issuance of an anticipatory search warrant, the affidavit should present strong evidence that the continuation of a process already initiated will result in sizeable arrival at a particular place at a particular time.

4.6 EXECUTION OF THE SEARCH WARRANT

Carrying out the search warrant by conducting the entry and search of the specified place is termed conventional search warrant execution. A search warrant is directed to a particular officer or class of officers. Only the named officer or a member of the named class of officers may execute or serve the warrant. If a warrant is directed to a sheriff, a deputy may execute the warrant and the sheriff need not be present. Officers may enlist private persons to help in the execution of a warrant, but an officer to whom the warrant is directed must be personally present at the search scene. The process of executing data processing by conducting forensic analysis is what is termed the virtual or cyber search warrant execution. The first step for the investigator is to begin the canvas in an attempt to locate or find the electronic or digital media that he or she believe has the highest likelihood or expectation of containing the evidentiary information described in the warrant. The execution of cyber search is conducted on-site, and therefore, mimics the stage of the traditional search procedures (Crimes and Criminal Procedures 18 USC § 3109; Crimes Act 1914).

The Cyber Search execution starts with the traditional or conventional search procedures which begin with the entry of the dwelling to search as to the entry of dwelling to arrest. Law enforcement officers should knock and announce their authority and purpose before entering the premises to execute a search warrant. Either way No-knock searches, searches without an announcement, may be authorized by state statute, particularly for drug cases. For example, In *Wilson v. Arkansas* 514 U.S. 927 (1995), the Court ruled that the “knock and announce common law principle is part of the Fourth Amendment’s

requirement that searches and seizures be reasonable." It added, however, that this did not mean that every entry should be preceded by an announcement. The current rule is that, although knock and announce is part of the requirement of reasonableness in searches and seizures, it is not a rigid rule and is subject to exceptions based on law enforcement interests.

An announcement of identity as a law enforcement officer accompanied by a statement that the officer has a search warrant is usually sufficient. A person who refuses entry to an officer executing a warrant risks forcible entry (*State v.Valentine*, 504 P.2d 84 [1972]). But officers who have knocked and announced their authority and purpose may enter forcibly until it is reasonably apparent that they are being refused entry. Refusal does not have to be explicit, but most commonly, is implied by an occupant's failure to admit officers within a reasonable time after they knocked and announced. The case of *United States v. Banks,* 124 S.Ct. 521. (2003), addressed the issue of what is a reasonable time for an occupant to respond. The law enforcement of the cyber search begins with notification and observes the physical location to be searched and then specifies the search method to identify the digital or electronic devices stated in the warrant. Documentation, recording, and video shots should be done to avoid contamination of evidence. According to the National Institute of Justice (2008) documentation of the scene creates a permanent historical record of the scene. Documentation is an ongoing process throughout the searching and seizing of hardware and software evidence. It is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence. Documentation of the scene should be created and maintained in compliance with departmental policy, and national, State, and local laws.

In addition, the National Institute of Justice Electronic Crime Scene Investigation guides for first responders (2008) state that the initial execution of a cyber search should begin with documentation of the physical scene which includes observing and documenting the physical scene, such as the position of the mouse and the location of components relative to each other (e.g., a mouse on the left side of the computer may indicate a left-handed user). In addition, the seizure of the hardware/physical containers involves labelling all

wires connected to the computer or devices and photographing the scene paying specific attention to the labelled connectors. The condition and location of the computer system including the power status of the computer, on, off, or in sleep mode. Most computers have status lights that indicate the computer is on. Likewise, if fan noise is heard, the system is probably on. Furthermore, if the computer system is warm, that may also indicate that it is on or was recently turned off. Law enforcement should identify and document related electronic components that will not be collected and photograph the entire scene to create a visual record (National Institute of Justice Electronic Crime Scene Investigation Guide for First Responders 2008). The complete room should be recorded with 360 degrees of coverage, when possible and the front of the computer as well as the monitor screen and other components should be photographed (National Institute of Justice Electronic Crime Scene Investigation guide for first responders, 2008). Also, take written notes on what appears on the monitor screen. Active programs may require videotaping or more extensive documentation of monitor screen activity (National Institute of Justice Electronic Crime Scene Investigation guide for first responders, 2008). The Movement of a computer system while the system is running may cause changes to system data. Therefore, the system should not be moved during the search until it has been safely powered down. It is important to shut down the computer system in a manner that will not damage the integrity of any files. Different operating systems have different shutdown procedures (National Institute of Justice Electronic Crime Scene Investigation guide for first responders, 2008). Some operating systems can be shut down by simply unplugging the power cord from the wall socket, while others have a more elaborate shutdown procedure. Anthony *et al* highlight that the most pressing issue relating to pull-the-plug is that some operating systems (OSes) really like to be shut down properly. Rapid power loss in some OSes can actually corrupt the operating system's kernel or the central module of the system. UNIX, Linux, and Macintosh operating systems are the most vulnerable, but some Windows-based OSes, such as a Windows 2000 server, should be shut down properly.

The EC-Council Investigation procedures and response (2016) outline the following procedures for shutting down or unplugging running computer systems:

A. MS-DOS/Windows 3.x/Windows 9x, Windows NT, Windows XP, Windows Vista, Windows, 7,8, and 10:

(i) Take a photograph of the screen,

(ii) Document any running programs

(iii) Unplug the power cord from the wall socket.

B. UNIX/Linux

(i) Right–click on Menu and click

(ii) If the root user is logged in, enter the password and type sync; sync; halt to shut down the system

(iii) If the root user is not logged in and the password is available, type su to switch to the root user, enter the password, and type sync; sync; halt to shut down the system.

(iv) If a password is not available, unplug the power cord from the wall socket.

C. Macintosh Operating System:

(i) Record the time from the menu bar

(ii) Click special and then Shut Down

(iii) Unplug the power cord from the wall socket

The chain of custody should be done at this stage to track the evidence collection from its original source to the courtroom presentation. The execution of cyber search for and collection of evidence at an electronic crime scene is relevant. Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value (NIJ Electronic Crime Scene Investigation Guide for First Responders, 2008).

This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation. The digital or recovery of non-electronic evidence can be crucial in the execution of cyber search and seizure. Proper care should be taken to ensure that such evidence is recovered and preserved. Law enforcement should collect evidence through the order of volatility (NIJ Electronic Crime Scene Investigation Guide for First Responders, 2008). The other collection should proceed from the most volatile

to the least volatile. Beginning with the most volatile such as registers and caches, to the routing table, process table, kernel statistics, and memory, to temporary files systems, then disk or storage media, remote logging and monitoring data that is related or significant to the system in question then physical configuration and network topology and lastly archival media. Items relevant to subsequent examination of electronic evidence may exist in other forms such as written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs and should be secured and preserved for future (NIJ Electronic Crime Scene Investigation Guide for First Responders, 2008).

4.6.1 Who May accompany the officers executing the Search?

Ferdico *et al* (2015:233) asserts that a search warrant is directed to a particular officer or class of officers. Only the named officer or a member of the named class of officers may execute or serve the warrant. If a warrant is directed to a sheriff, a deputy may execute the warrant and the sheriff need not be present. Officers may enlist a private person to help in the execution in the execution of a warrant, but an officer to whom the warrant is directed must be personally present at the search scene. For example, in the United States, it is a violation of the Fourth Amendment for police to bring members of the media or other third parties into a home during the execution of a warrant when the presence of the third parties in the home was not in aid of the execution of the warrant.

In the matter of *Wilson v. Layne,* 526 U.S. 603 (1999), the Supreme Court decision held that the Fourth Amendment protection against unlawful search and seizures prohibited the police from bringing members of the news media into private homes while executing search warrants. Virtual crime or digital crimes have extraordinary phases in their search execution and require digital tools and conventional searches to accomplish the desired results together with a team of investigators such as technicians, evidence custodians, forensic examiners, forensic analysts and electronic discovery experts. Usually, they have the first responders who create a toolkit before a cybercrime event happens and prior to

any potential evidence collection. Once a crime is reported, someone should immediately report the site and should not have to waste any time gathering materials. The first responder toolkit is a set of tested tools designed to help in collecting genuine presentable evidence. The first responder has to select trusted computer forensic tools that provide output-specific information and determine system dependencies. Since there are complex and difficulties in digital investigations, there is always a professional investigator who is trained to conduct all complex cybercrimes and conduct the traditional searches and deal with real suspects.

4.6.2 The Time Allowed for a Search

The search cannot last indefinitely, with or without a warrant. Once the item mentioned in the warrant is recovered, the search must cease (Carmen 2013:216). Three different aspects of time affect law enforcement and investigators in the execution of search warrant (Ferdico *et al* 2015:231), first is the allowable delay between the warrant's issuance and its execution, secondly the time day during which the warrant may be executed, and the amount of time allowed for the law enforcement officer to perform the search once it is initiated. In jurisdictions with no time limit fixed by statute, court rule, or judicial decision, a warrant must be executed within a reasonable time after issuance. Some jurisdictions require that a search warrant to executed and returned within ten days after its date of issuance. These jurisdictions may also require that the warrant be executed forthwith. To resolve this apparent ambiguity, courts require that the warrant be executed within a reasonable time after issuance. Scheb and Scheb (2011:448) state that the US State of Texas allows three days, excluding the date of issuance and the date of execution, Veron's Ann. Texas C.C.P. Art. 18.07, whereas California allows ten days, West's Ann. Cal. Penal Code § 1534. Likewise, some countries' or states' laws vary on the hours during which a search warrant may be executed. California law provides that upon a showing of good cause, the magistrate may, at his or her discretion, insert a direction in a search warrant that it may be served at any time of the day or night. In the absence of such a direction, the warrant shall be served only between the hours of 7 a.m. and 10 p.m. West's Ann. Cal. Penal Code § 1533. Some states in the United States, including Texas, do not impose restrictions on the hours when a warrant may be

executed; others allow nighttime searches under special circumstances (Scheb & Scheb 2014:440).

Carmen and Hemmens (2017:230) state that a continued search without justification becomes a fishing expedition for evidence and is illegal. An illegal search is never made legal by what is subsequently found. For example, suppose the police go to an apartment to execute a search for a shotgun allegedly used in a murder. After the shotgun is recovered, the police continue to search for other evidence in connection with the murder. They open a bedroom closet and find a pair of bloodied jeans worn by the suspect during the murder. The bloodied jeans, if seized and used in evidence, will not be admissible, because they were illegally obtained.

4.7 SEARCHING AND SEIZING WITHOUT WARRANT

Carmen (2013:237) indicate that in searches and seizures without a warrant, the burden is on the law enforcement or the investigator to prove in court that probable cause existed at the time of the warrantless search or seizure. It is therefore essential for law enforcement officers to be thoroughly familiar with the law on warrantless searches and seizures.

Marras (2015:89) indicate that certain exceptions that justify a search without a warrant include:

(a) The searches incident to lawful arrest" exception
(b) The "searches with consent" exception
(c) The "exigent circumstances" exception
(d) The Border Searches
(e) Plain View Doctrine

4.7.1 Searches Incident to Lawful Arrest and Exception

Searches that occur upon the arrest of individuals encompass searches of the arrestees and the areas under their immediate control. Ferdico *et al* (2015:372) state that the search incident to lawful arrest exception is widely used in policing. It is invoked almost every time an officer makes an arrest, with or without a warrant. There are three justifications for warrantless searches incident to arrest: (1) to ensure officer safety, (2) to prevent escape, and (3) to prevent concealment or destruction of evidence. The authorization to search incident to arrest is always available to the officer after an arrest, even if there is no probable cause to believe it is necessary to ensure officer safety, to prevent escape, or to prevent concealment or destruction of evidence. These searches take two forms: body search and search of the area within the person's immediate control.

The body search is valid in any situation in which a full-custody arrest of a person occurs. There is no requirement that the officers fear for their safety or believe that they will find evidence of a crime before the body search can be made (*United States v. Robinson,* 414 U.S. 218 [1973]).In addition to performing a body search, the officer may also search the area within the person's immediate control. The leading case on this issue is *Chimel v. California* 395 U.S. 752. (1969), in Chimel, the Court said: When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's per son in order to prevent its concealment or destruction. The Supreme Court has carved out, comparatively recently, a series of exceptions to the warrant requirement, collectively known as the "special needs beyond law enforcement" exception. What these situations have in common is that they are not police searches (although sometimes the police are asked to help) but instead involve searches conducted by other public agencies that perform tasks related to law enforcement. Examples are school searches, searches of probationers and parolees, and airport searches. The Court has repeatedly held that these types of searches may be made without a warrant and on less than probable cause. This section looks at each of the examples.

Public School Searches in *New Jersey v. T.L.O.* 469 U.S. 325 (1985), the Court resolved an issue that had long bothered public school students, teachers, and administrators. Voting 6 to 3, the Court said that public school teachers and administrators do not need a warrant or probable cause to search a student they believe is violating the law or school rules. In the matter of *Griffin v. Wisconsin*, 483 U.S. 868 (1987), The Court added that the supervision of probationers is a "special need" of the state that justifies a departure from the usual warrant and probable cause requirements. In *United States v. Davis* 482 F.2d 893 (9th Cir. 1973), the court said, that "the need to prevent airline hijacking is unquestionably grave and urgent. A pre-boarding screening of all passengers and carry-on articles sufficient in scope to detect the presence of weapons or explosives is reasonably necessary to meet the need.

4.7.2 Consent Search

Marras (2015:91) indicates that one of the most relevant exceptions to the requirements for a warrant to conduct the search and seizure of computers is the consent search. According to the ruling in *Schneckloth v. Bustamante,* consent searches are part of the standard investigatory techniques of law enforcement agencies. Ferdico *et al* (2015:372) assert that consent search occurs when a person voluntarily waives his or her privacy rights and allows a law enforcement officer to search his or her body, premises or belongings. Consent searches normally occur on the highway, or in a person's home or office, and under informal and unstructured conditions. Search can occur without a warrant and without probable cause if an individual who has authority over the place or items to be searched has consented to the search (*Stoner v. California,* 376 U.S.483 [1964]); (*United States v. Matlock,* 415U.S. 164, 171 [1974]). For consent search to be legal, the individual, must not have been tricked or coerced into consenting to the search. If an individual consents to a search when a law enforcement agent falsely claims to have a warrant to search the premises, the Court will found the consent invalid and will deemed the search unconstitutional (*Bumper v. North Carolina,* 391 U.S.543, 550. [1968]).

A consent search can benefit a consenting party who is innocent of any wrongdoing. In *Schneckloth v. Bustamonte* 412 U.S. 218, 228 (1973), the court held that during the course of a consent search of a car that had been stopped by officers for traffic violations,

evidence was discovered that was used to convict respondent of unlawfully possessing a check. In a habeas corpus proceeding, the Court of Appeals, reversing the District Court, held that the prosecution had failed to prove that consent to the search had been made with the understanding that it could freely be withheld. A perennial problem in the area of consent searches is that of third-party consent. The problem is especially acute in situations where several persons share a single dwelling, but many Court have said that the consent of a third party is valid only when there is mutual use of the property by persons generally having joint access or control. The *United States v. Matlock,* 415U.S. 164, 171 (1974) case stands for the principle that the validity of third-party consent is tested by the degree of dominion and control exercised by the third party over the searched premises and that a joint occupant may provide valid consent only if the other party is not present." and is depicted in Figure 4.9. below.

CONSENT TO SEARCH
(See JAGMAN 0170)

I, _____, have been advised that inquiry is being made in connection with _____. I have been advised of my right not to consent to a search of [my person] [the premises mentioned below]. I hereby authorize

_____

and _____, who [has] [have been] identified to me as

_____ to conduct a complete search of
Position(s)

my [person] [residence] [automobile] [wall locker] [_____] located at

_____

_____.

I authorize the above listed personnel to take from the area searched any letters, papers, materials, or other property which they may desire. This search may be conducted on _____.
Date

This written permission is being given by me to the above named personnel voluntarily and without threats or promises of any kind.

_____
Signature

WITNESSES

_____

_____

- Figure 4.9. A suggested Consent to search form. Source JAG Manual

In *Illinois v. Rodriguez,* 497 U.S. 177 (1990), the Supreme Court shifted the focus from the dominion and control of the third party to the police officer's subjective belief that the third party has the authority to grant consent to a search of the premises. Writing for the Court, Justice Antonin Scalia opined that a warrantless entry is valid when based on the consent of a third party that the police reasonably believe to possess common authority over the premises, even if the third party does not in fact have such authority. There are a number of well-established situations in which third-party consent is not valid Scheb & Scheb (2014:436). Tenancy arrangements are a good example. A landlord does not have the implied authority to consent to the search of a tenant's premises. *Chapman v. United States*, (365 U.S. 610.1961). Likewise, a hotel manager or clerk does not have the right to consent to the search of a guest's room during the time the guest has a legal right to occupy the room (*Stoner v. California*, 376 U.S. 483, (1964). Finally, consent to search may be revoked "prior to the time the search is completed" (*United States v. Lattimore,* 87 F.3d 647, 651 (4th Cir. 1996). When agents obtain consent to remove computers for off-site review and analysis, the time required for review can be substantial. In such cases, law enforcement should keep in mind that before incriminating evidence is found, the consent may be revoked.

The scope of consent to search is "generally defined by its expressed object, and is limited by the breadth of the consent given" (*United States v. Pena,* 143 F.3d 1363 [10th Cir. 1998]). Computer cases often raise the question of whether general consent to search a location or item implicitly includes consent to access the memory of electronic storage devices encountered during the search. In such cases, courts look to whether the particular circumstances of the agents' request for consent implicitly or explicitly limited the scope of the search to a particular type, scope, or duration. Compare *United States v. Reyes,* 922 F. Supp. 818 (1996) (consent to "look inside" a car included consent to retrieve numbers stored inside pagers found in car's back seat), with *United States v. Blas,* (1990 WL 265179) (consent to "look at" a pager did not include consent to activate pager and retrieve numbers, because looking at pager could be construed to mean "what the device is, or how small it is, or what brand of pager it may be").

4.7.3 The exigent searches

The exigent circumstances exception is a general catchall category that encompasses a number of diverse situations. What they have in common is some kind of an emergency that makes obtaining a search warrant impractical, useless, dangerous, or unnecessary. Among these situations are the danger of physical harm to the officer or destruction of evidence, searches in hot pursuit, danger to a third person, and driving while intoxicated. In *United States v. David* 756 F. Supp. 1985 (D. Nev. 1991), the court stated that evidence can be seized without a warrant if the destruction of the evidence is imminent and there is probable cause to believe that the item seized constitute evidence of criminal activity. Generally, emergency circumstances arise with computers and mobile phones if suspects seek to damage the computer or mobile phones or delete its files. Usually, this exception allows a law enforcement agent to seize a computer or other electronic device. The search of the device, however, usually requires another search warrant.

For example, in *United States v. David* 756 F. Supp. 1985 (1991), the law enforcement agent seized the defendant computer memo book because the defendant was deleting files in it. After the memo book was seized from the suspect possession, the law enforcement agent was required to obtain a warrant to search it. Sometimes emergence access to electronic devices is required because evidence may be destroyed independent of any action by the suspect. In *United State v. Parada* 03-40053-01-JAR (2013), the defendant cell phone records were accessed because of exigent circumstances. Specifically, swift access to these records was required because incoming calls had the potential of overwriting call memory, thereby possibly destroying vital evidence in the case. The Court has implied that a warrantless search may be justified if there are reasonable grounds to believe that delaying the search until the warrant is obtained would endanger the physical safety of the officer or would allow the destruction or removal of the evidence (*Vale v. Louisiana,* 399 U.S. 30 (1970). However, in *Vale v. Louisiana,* 399

U.S. 30 (1970), the Supreme Court did not allow a warrantless search when there was merely a possibility that the evidence would be destroyed.

4.7.4 Application of Boarder Searches Doctrine

Each sovereign nation has the right to regulate the entry and exit of individuals at its borders and under what entry and exit of individuals at its borders and under what condition this may occur. In most cases, many courts have found warrantless border searches reasonable primarily because of the belief that the sovereign nation has the right to protect itself by stopping and examining persons and property crossing into this country (*United States v. Flores-Montano,* 541 U.S.149, 152-153 (2004).). The interests of the sovereign state to exclude undesirable persons and prohibited goods have been cited to justify warrantless searches and searches conducted without reasonable suspicion or probable cause (*United States v. Flores-Montano,* 541 U.S.149, 152-153 [2004]). Although routine border searches do not require reasonable suspicion, probable cause, or a warrant (*United States v. Montoya de Hernandez* 473 U.S 531, 538 473 U.S 531, 538 [1985]), the same cannot be said about non-routine searches. The courts have ruled that reasonable suspicion is required for the detention of a traveler at the boarder beyond the scope of a routine customs search and inspection (*United State v. Sandoval vargas,* 490 U.S. 854 [1998]). Thus any non-routine search must be preceded by reasonable suspicion of criminal activity and the search must not exceed that which is necessary to find the evidence of the crime (*United States v. Couch,* 688 F2d 599, 604 [9th Cir. 1982])

In United *States v. Roman* 917 F. 3d 1043 (2019), the defendant flew from United State to Canada. Upon arriving in Canada, he was questioned by agents from Canada's Boarder Services Agency concerning the criminal history. The agent also checked his computer and found several child pornography websites listed in his Internet history. Roman was denied entry to Canada detained, and subsequently sent back to the United States. Upon his arrival in the United States, his computer was searched again, and the evidence retrieved from it was used to charge Roman with crimes related to child pornography. Roman sought to have the evidence suppressed by claiming that the search and seizure of his computer violated his rights under the United States Fourth

Amendment. The court disagreed, holding that international airports are the functional equivalent of a boarder and therefore, the search *Romm's* computer fell within the scope of the border search exception (*United State v. Romm,* 455 F3d 990, 997 [2006]). Also, in *United States v. Arnold* (454 F. Supp. 2d 999*)* the defendant was selected for secondary questioning at the Los Angeles International airport after arriving from the Philippines. Upon inspecting his luggage customs officials found a laptop computer, a hard drive, a computer memory sticks, and six CDs. A customs official asked Arnold to turn the computer on, which he did. The Customs official believed warranted the attention of special agents from U.S. Immigration and Customs Enforcement (ICE). Subsequently, the ICE special agents searched Arnold's laptop and found what they believe to be child pornography. The special agents then seized Arnold's laptop and storage devices. According to Arnold, the warrantless search of evidence retrieved from his laptop and storage devices should be suppressed. Although the District Court of the Central District of California agreed with him by finding that the search and seizure of Arnold's laptop by customs agents violated the Fourth Amendment, this decision was later overturned by the Ninth Circuit Court of Appeals. The courts have rendered similar judgements, upholding warrantless searches under the border exception, in other cases involving the transport of child pornography (*United States v.Ickes* 393 F3d, 501,503 4th Cir.[2005])

4.7.5 The plain view doctrine

According to Sady (2012:25), the plain view doctrine is a legal concept deduced from three landmark decisions, *Coolidge v. New Hampshire* 403 U.S. 443 (1971); *Arizona v. Hicks* 480 U.S. 321 (1987); and *Horton v. Californi* 496 U.S. 128 (1990). Jarrett and Bailie (2009:38) conclude the plain view means evidence in plain view of the investigator who has a right to search may be seized. Kerr (2013:567) states plain view means "unpredictably locating evidence, without possessing prior knowledge that such evidence existed in that location and without executing any physical search to find it." Plain view concept occurs during execution of a search warrant when evidence not mentioned in the search warrant surfaces and is seized. Brooks (2004:101) asserts that there is a challenge with plain view doctrine in relation to computer-related crime." This is because

the documents, files and databases stored in computers are intermingled and are either latent or active

The plain view doctrine states that items that are within the sight of an officer who is legally in the place from which the view is made may properly be seized without a warrant—as long as such items are immediately recognizable as subject to seizure. In the words of the Court, “It has long been settled that objects falling in the plain view of an officer who has a right to be in a position to have that view are subject to seizure and may be introduced in evidence” (*Harris v. United States*, 390 U.S. 234)

Kerr (2013) advanced three methods which might limit the applicability of plain view doctrine in computer searches and posits that forensic tools diminish the plain view doctrine, plain view doctrine will be accepted where the crime is serious and that annihilation of the plain view doctrine in computer crime-related searches poses challenges when applied in digital environment. On the other hand, United States Department of Justice Search and Seizure Manual (2002) argue that, the plain view doctrine may be applicable in digital searches if the following are adhered to:

(a) The source of evidence should be accessed legally by including in the search warrant the nature of electronic storage and the desire to examine the entire contents of the device.
(b) The apparent illegal nature of the evidence is immediately known, for example, in the investigation of a Disk Operating System (DoS) attack; the investigator can seize pornography images displayed on the computer’s screen.
(c) The investigator should not abandon the original search.

Brooks (2004:74) further highlights that, in computer searches, whether it is not immediately clear that evidence retrieved falls within the scope of the search warrant, the investigating officer has to carry out further examination to establish that. The plain view doctrine has been applied to cybercrime cases where the search is a computer pursuant to a valid warrant subsequently led to the discovery of incriminating information not specified in the warrant. For example, in *United States v. Carey,* the warrant specified

that law enforcement personnel could search the suspect's computer for documentary evidence pertaining to the sale and distribution of controlled substance. While searching the suspect computer for evidence of the sale and distribution of drugs, the investigator found images of child pornography. The investigator then abandoned the initial search for drugs files and started searching for more child pornography images. However, every image after the initial discovery of an image of child pornography was ruled inadmissible in court. This is because if incriminating evidence other than that specified in the warrant is found during a search, the investigator should stop the search and get a new warrant based on the plain view evidence discovered. Again, in *United States v. Wong,* (334 F.3d 831, 838 9th Cir.), an agent discovered child pornography on a hard drive while conducting a valid search of the drive for evidence of a murder. Because the agent was properly searching graphics files for evidence of the murder, the child pornography was properly seized and subsequently admitted under the plain view doctrine. The plain view doctrine can also be useful in other circumstances when agents are lawfully in a position to discover incriminating evidence on a computer.

4.8 RESPONSES OF DIGITAL SEARCH AND SEIZURE FROM THE COUNTRIES UNDER STUDY

4.8.1 Ghana Legal response to searching and seizing digital evidence

Probable or reasonable cause has been clearly specify or formed into a corporation in the Ghanaian legislation for conventional searches. The Criminal Procedure Act 30 of (1960) provides extreme magnitude for issuing a search warrant. Section 88 (1a, b, c) states that, a District Magistrate who is satisfied, by evidence upon oath, that there is reasonable ground for believing that there is in any building, vessel, carriage, box, receptacle, or place or :

(i) anything upon or in respect of which any offence has been or is suspected to have been committed, for which according to any law

for the time being in force, the offender may be arrested without warrant; or

(ii) anything which there is reasonable ground for believing will afford evidence as to the commission of any such offence; or

(iii) anything which there is reasonable ground for believing is intended to be used for the purpose of committing an offence against the person for which, according to any law for the time being in force, the offender may be arrested without warrant, may at any time issue a warrant under his hand authorising any constable to search any such building, vessel, carriage, box, receptacle, or place for any such thing, and to seize and carry it before the Magistrate issuing the warrant or some other Magistrate to be by him dealt with according to law.

In addition, section 89 specifies the time when search warrant may be executed and it state that every search warrant may be issued and executed on a Sunday and shall be executed between the hours of 6.30 a.m. and 6.30 pm., but the Court may, by the warrant, in its discretion, authorize the police officer or other person to whom it is addressed to execute it at any hour. However, at the time of writing the researcher found out that there is no documented court cases that addressed the issue of Internet Protocol (IP) address and probable cause. All addressed made on probable cause by scholars and expert concerns conventional searches. No provisions in the legislations specifically deal with cyber searches mirror copy and there is no scholarly work identify and analysis the issue. In addition, there are no court decisions on cyber searches and mirror copy. With this in place, it is highly that conventional search warrant procedures would be applied to cyber searches. The Criminal Procedure Act 30 of (1960) provides threshold for issuing a search warrant, and executing officers to search and seize any material items that are tangible and might relate to any offense.

Currently, the laws of Ghana authorize search of and seizure of things that are tangible. Article 18 of the Ghanaian Constitution deal with individual protection of privacy of home and other property in Ghana. Section 2 of (Article 18) of the Ghana Constitution state that: No person shall be subjected to interference with the privacy of his home, property, correspondence or communication. In addition, the constitution protect unreasonable or illegitimate search of physical places used for residential purposes, such as hotels, guest houses, private apartments. However, the virtual or digital contents were not addressed by the law and not identify as an article or item their own right. On the other hand, the Criminal Procedure Act 30 of (1960) identifies that the subject of the search warrant is either physical place, building in which a person lives and maintain privacy, or vessel, carriage, box, receptacle that items are kept. In addition the Section 88 (A and B) of the criminal Procedure Code 1960 (Act 30) authorize the police to seize anything which there is reasonable ground for believing will afford evidence as to the commission of any such offence or anything which there is reasonable ground for believing is intended to be used for the purpose of committing an offence against the person for which, according to any law for the time being in force, the offender may be arrested without warrant.

In Ghana, the judge or magistrate is the only authority entitled to prepare and issue search warrants. The judge or magistrate issue search warrant to the police officers to execute it. However, the officer designated to execute search warrant must all time obey and adhere to the judge or magistrate instructions about the warrant execution procedures, its scope, location or area to be searched, its time or day the search should be executed. The warrant must be performed according to the rules of laws governing the search and seize. In regard to the pre-digital search phase, the Criminal Procedure Act 30 of (1960)) gives powers to the judge or magistrate to issue search warrant to the police or law enforcement to search without notifying in advance the defendant or the suspect of the search. The defendant or his representative can be present during the time of search warrant execution. The Act also gives powers to judge or magistrate to issue broad discretion which concerns the appropriate procedures and measures that the law enforcement or the investigators follow to ensure proper search and seizure operation. However, the digital phase has no legal provisions that address the particular procedures

or methods for searching and seizing computer artefacts. Even though there are no provisions concerning cyber searches, conventional search execution requirements must be observed when executing cyber search. The Judge can nominate an expert such as digital forensic investigators, to provide assistance and the expert must declare under oath that they will carry out their task in trustful manner and impartially.

4.8.2 United States(US) Legal responses to searching and seizing digital evidence

The fourth amendment does not prohibit all searches and seizures, only those that are unreasonable (Ferdico *et al* 2015:139). The Fourth Amendment protect the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. In *Beck v. Ohio 379 U.S.89 (1964*) the court stated that officers had probable cause to make it whether at that moment the facts and circumstances within their knowledge and of which they had reasonably trustworthy information were sufficient to warrant a prudent man in believing that the petitioner had committed or was committing an offence. Probable cause is evaluated by examining the collective information in the possession of the police at the time of the arrest or search, not merely the personal knowledge of the arresting or searching officer. In *United States v. Thevis* 469 F.Supp.490(1979), the court stated that law enforcement officers in diverse jurisdictions must be allowed to rely on information relayed from officers and or law enforcement agencies in different localities in order that they might coordinate their investigations, pool information, and apprehend fleeing suspect in today's mobile society. In order to satisfy the reasonableness requirement of the Fourth Amendment, government agents need not always be correct, but they must always be *reasonable (Illinios v. Rodrigues,* 497 U.S. 177, [1990]).

The law enforcement officers or investigators plays a significant role in establishing a strong probable cause, thus it is helpful to begin search warrant affidavit with an introductory paragraph that briefly describes the officer's training and experience in the area or subject matter of the investigation. If law enforcement officer knowingly and

intentionally, or with reckless disregard for the truth, makes false statements in an affidavit supporting a request for a search warrant, the warrant may not issue and if the warrant does issue, evidence seized under the warrant may be suppressed. In *Franks v. Delaware,* 438 U.S. 154 (1978), the court held that a defendant may challenge the veracity of an affidavit used by the police to obtain a search warrant. This was also supported in *United States v. Pace,* 898 F2d 1218 (1990) where the court found that the *Franks* rule also probihits an officer from deliberately or recklessly omitting material information from a warrant application. If a warrant application is so lacking in indicia of probable cause as to render official belief in its existence unreasonable, the officer making the application may be held liable for damages in a civil suit (*Malley v. Briggs,* 475 U.S. 335 [1986]).

The Fourth Amendment and the Privacy Protection Act (PPA) protect materials and defend individual against broad search and seizure. Search warrant must specify the particular areas to be searched. Determination of the scope of a search involves issues of whether permission to actually search, rather than merely enter, has been given and what limits are place on the search in terms of area, time, and expressed object of the search. Mere reference to evidence of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize. The Fourth Amendment “is wholly inapplicable to a search or seizure, even an unreasonable one, affected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official,” held the court in *United States v. Jacobsen*, 466 U.S. 109, [1984]). As a result, no violation of the Fourth Amendment occurs when a private individual acting on his own accord conducts a search and makes the results available to law enforcement. Government acquisition of an intangible electronic signal in the course of transmission may also implicate the Fourth Amendment (*Berger v. New York,* 388 U.S. 41, 58-60). The boundaries of the Fourth Amendment in such cases remain hazy, however, because Congress addressed the Fourth Amendment concerns identified in Berger by passing

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2510-2522.

Data stored on electronic device are recognize by the United States courts. The Electronic Communication Privacy Act of 1986 (ECPA) for example, authorizes law enforcement officers to access and seize digital data stored by a provider electronic communications services. According to the Supreme Court, a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property," *United States v. Jacobsen,* 466 U.S. 109, 113 [1984]) and the Court has also characterized the interception of intangible communications as a seizure. Also in a matter of *Berger v. New York,* 388 U.S. 41, (1967). Real-time electronic surveillance in federal criminal investigations is governed primarily by two statutes. The first is the federal Wiretap Act, 18 U.S.C. §§ 2510-2522, first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and generally known as "Title III"). The second statute is the Pen Registers and Trap and Trace Devices chapter of Title 18 ("the Pen/Trap statute"), 18 U.S.C. §§ 3121-3127, first passed as part of the Electronic Communications Privacy Act of 1986. Failure to comply with these statutes may result in civil and criminal liability, and in the case of Title III, may also result in suppression of evidence.

However, in United *States v. Payton,* F.3d 2009 WL 2151348, (2009), the Ninth Circuit held that law enforcement is not necessarily entitled to examine a computer that may contain evidence that falls within the scope of a warrant. In *Payton*, an officer executing a search warrant that authorized a seizure of drug sales records and other financial records searched a computer capable of storing such records. The court held that because the warrant did not specifically authorize a search of the computer, and because nothing else present at the scene of the search suggested that records falling within the scope of the warrant would be found on the computer, the search violated the Fourth Amendment. Under Payton, it is good policy for prosecutors and agents seeking a warrant in the Ninth Circuit to always seek specific authorization to search computers, though failure to do so will not necessarily invalidate the search.

4.8.3 United Kingdom Legal responses to searching and seizing digital evidence

The Police and Criminal Evidence Act 1984 is an Act of Parliament which instituted a legislative framework for the powers of police officers in England and Wales to combat crime, and provided codes of practice for the exercise of those powers (Police and Criminal Evidence Act 1984). Nieman (2009:311) assert that the law governing the preservation, production and search and seizure of electronic evidence in England has four primary sources. The Police and Criminal Evidence Act (Part I) Sections1 to 7 provide law enforcement officers with powers to stop and search. The (part II) of Sections 8 to 23 of Police and Criminal Evidence Act also provide impart general powers of entry, search and seizure. Furthermore, the Criminal Justice and Police Act (CJPA) 2001 Sections 50 and 51 allow for the seizure and removal of property found on premises or on a person where it is not reasonably practicable to complete a process of examination, searching or separation at the scene. Section 50 refers to seizure from premises section 51 refers to seizure from a person.

Powers of arrest without a warrant can be exercised by a constable who 'has reasonable grounds' to suspect that an individual is "about to commit an offence", or is "committing an offence"; in accordance with the Serious Organised Crime and Police Act 2005 and the partially repealed Police and Criminal Evidence Act 1984. The concept of "reasonable grounds for suspecting" is used throughout the law dealing with police powers. Also, sections 21 to 25 of the Regulation of Investigatory Powers Act (RIPA) are aimed at the acquisition and disclosure of communications data, including traffic data. Sections 49 to 56 of this Act also introduce a power to require the disclosure of protected data in an effort to maintain the effectiveness of existing law enforcement powers in the face of the increasing criminal use of encryption Thirdly, it is important to bear in mind that the retention of data is closely associated with the provision and accessing thereof and retained data is preserved by default. The retention of communications data in England is currently addressed by the voluntary code of practice on the retention of

communications data issued by the Home Secretary in 2003 under authority of the Anti-Terrorism, Crime and Security (Act 9).

Nieman (2009:314) posit that the main innovation effected by PACE was the creation of powers of search and seizure that are not offence-specific, but are instead to be exercised according to statutory criteria that attempt to maintain a balance between crime control and civil liberty. These powers include the right to stop and search a person and her property prior to arrest (sections 1-3 of PACE and its Code of Practice A), to effect road checks(sections 4 and 5 of PACE and PACE Code of Practice A),to apply for a warrant to a justice of the peace(Sections 8, 15 and 16 of PACE), to make a warrantless search of persons and of premises on arrest(sections 18 and 32 of PACE and the PACE Code of Practice B), and to apply to a circuit judge for a production order or a warrant to obtain sensitive and/or confidential material(sections 9, 11-14 and Schedule 1 of PACE and the PACE Code of Practice B). Most of the powers to authorise searches prior to the promulgation of PACE are retained, so the earlier law has been supplemented, rather than changed (section 8(5) of PACE).

The Police and Criminal Evidence Act 1984 (PACE) Codes of Practice are set out under eight different sections labelled A to H. Each deal with a different aspect of the police's duties as follows: The PACE Code A deals with a police officer's legal powers to search a person and or any vehicle prior to making any arrest. They must also make a note of the encounter. Police and Criminal Evidence Act (1984) Code B outlines the police's powers to enter and search premises and seize any possessions found on a person or premises. The powers under this code are conferred to find anyone wanted by police for questioning, arrest or, in relation to any crime; to find any property and material relating to the commission of a crime or; to find any children who should be in local authority custody where they have been remanded or placed following a court order. Police and Criminal Evidence Act (1984) Code B section1 (3a) outlines powers to search and seize must be used fairly, responsibly, with respect for people who occupy premises being searched or are in charge of property being seized and without unlawful discrimination. The Equality Act 2010 makes it unlawful for police officers to discriminate against, harass

or victimize any person on the grounds of the ‘protected characteristics’ of age, disability, gender reassignment, race, religion or belief, sex and sexual orientation, marriage and civil partnership, pregnancy and maternity when using their powers. When police forces are carrying out their functions they also have a duty to have regard to the need to eliminate unlawful discrimination, harassment and victimisation and to take steps to foster good relations.

Section 47(a) of the Terrorism Act 2000 allows police to stop and search someone or a vehicle, without reasonable suspicion, in order to prevent acts of terrorism. Searches under this power may only be authorised by a senior police officer, in a specific area for a defined period where the police reasonably suspect an act of terrorism will take place. Section 43 of the Terrorism Act 2000 Under Section 43 of the Terrorism Act 2000, police have the power to stop and search an individual if they have a reasonable suspicion that they have in their possession something which would constitute evidence that they are involved in terrorist activities. Schedule 7 of the Terrorism Act Schedule 7 of the Terrorism Act 2000 allows examining officers (police, immigration or custom officers) to stop and search individuals at airports, shipping ports or international rail terminals, for the purpose of determining whether an individual is or has been concerned in the commission, preparation or instigation of acts of terrorism. The Criminal Procedure and Investigations Act 1996 is a piece of statutory legislation in the United Kingdom that regulates the procedures of investigating and prosecution of criminal offences.

4.8.4 Australia Legal responses to searching and seizing digital evidence

Brown (2015: 48) indicated that a reasonable and probable ground most prominently regulates police officers as a precondition of the exercise of certain powers in their function as enforcers of the law. The *law enforcement Power and responsibilities act 2002* section 87 states that police officer who enters a dwelling under a power conferred by or under this Act and who believes, on reasonable grounds, that--(a) a dangerous article or dangerous implement (other than a laser pointer) is in the dwelling, and(b) that the dangerous article or dangerous implement is being, or was, or may have been or may be used to commit a domestic violence offence, may search the dwelling for

the dangerous article or dangerous implement and seize and detain the dangerous article or dangerous implement. *The Crime Act 9114*, Division 2 (3E) (1) An issuing officer may issue a warrant to search premises if the officer is satisfied, by information on oath or affirmation, that there are reasonable grounds for suspecting that there is, or there will be within the next 72 hours, any evidential material at the premises. *The Crime Act 9114, 3E(5*) also Provides: If an issuing officer issues a warrant, the officer is to state in the warrant:

(a) The offence to which the warrant relates; and
(b) A description of the premises to which the warrant relates or the name or description of the person to whom it relates; and
(c) The kinds of evidential material that are to be searched for under the warrant; and
(d) The name of the constable who, unless he or she inserts the name of another constable in the warrant, is to be responsible for executing the warrant; and
(e) The time at which the warrant expires (see subsection (5A)); and
(f) Whether the warrant may be executed at any time or only during particular hours.

In *R v Peirson* [2014] QSC 134, the court held that the evidence of the seizure of the mobile phone and the evidence obtained as a result of its having been taken from Mr Peirson, including evidence from witnesses who have been approached for and provided statements about his dealings with them on the basis of the information contained in the mobile phone, is admissible at his trial. The issue for determination is whether the mobile phone was legally searched by the police officer who spoke to him that evening pursuant to s 29 and s 30 of the Police Powers and Responsibilities Act 2000 (Qld). Commonwealth Parliament (2019) assert that criminal law is a state-law matter, as State and Territory Governments are mandated under their respective constitutions to legislate for the peace, order, and good government of their respective jurisdictions But, while there is no general constitutional basis for the Commonwealth to legislate in criminal law, federal legislation

exists to deal with crimes of a federal nature Commonwealth Parliament (2019). This has happened, for example, in the areas of corporation's regulation (2001) and anti-terrorism legislation (2002). For instance, The *Crimes Act* 1900 is a New South Wales statute that sets out the majority of criminal offences for the state of New South Wales in Australia. Along with the Crime Act 1914 and the Federal Criminal Code Act 1995 (both federal), these three pieces of legislation form the majority of criminal law for New South Wales. Also in *R v Varga* [2015] QDC 82 the court held that Evidence of SMS text messages and admissions and confessions by the accused with respect to the charges of trafficking in, and supply of, a dangerous drug and possession of a thing used in connection with trafficking in a dangerous drug, was lawfully obtained and is admissible.

The Australian Crimes Act 1914 Section 3F (1) draws the limits of the search scope and state that the warrant should be issued to search the premises for the kinds of evidential material specified in. The Crimes Act 1914 Section 3(C) defines "evidential material" as a thing relevant to an indictable offense or a thing relevant to a summary offence, including such a thing in electronic form.' The Section 3(F) conclude that executing officers are obliged to search and seize the items listed on the search warrant, including. The Crimes Act 1914 empowers the executing officers to make a mirror copy. The sections 3(F), 3(K), and 3(L) provide executing officers with a variety of options:

(a) Bringing to the warrant premises forensic equipment to examine or process data in order to determine whether it may be seized
(b) Removing from the premises data to examine or process elsewhere in order to determine whether it may be seized (Crimes Act 1914 (Cth) div. 2s 3L (2)
(c) Operating electronic equipment at the premises, copying the data found thereby on to a device brought to the premises and removing that device from the premises. (Crimes Act 1914 (Cth) div. 2s 3L (1a)
(d) Operating electronic equipment at the premises and then seizing it (Crimes Act 1914 (Cth) div. 2s 3L (2a)

(e) Operating electronic equipment at the premises, using facilities at the premises to create documents there-from and then seizing them. (Crimes Act 1914 (Cth) div. 2s 3L (2b)

(f) Securing electronic equipment at the premises so that it may be operated with the assistance of an expert. (Crimes Act 1914 (Cth) div. 2s 3L (4b)

These provisions empower executing officers to search unsystematically or rummage through data first and then make mirror copy and seize specified evidential material. In *Kennedy v. Baker*, for example, the Australian Federal Court permitted the executing officer to conduct and remove the hard drive image from the premises. The explanatory Memorandum to the Cybercrime Bill 2001 explained subsection 3L. It stated that:

> "It would enable law enforcement officers executing a search warrant to copy data held on any electronic equipment or associated devices at search premises to a storage device where there are reasonable grounds for suspecting that the data contains evidential material. These will permit contains evidential material or if there are reasonable grounds to suspect the data contains evidential material….. The existing provision only allows evidential material to be copied (Crimes Act, paragraph 3L (2c). Electronic equipment, such as a computer hard drive, can hold large amount of data. It is often not practicable for officers to search all the data for evidential material while at the search premises and to then copy only the evidence material which is found. The proposed provision would allow officers to copy all the dta on a piece of electronic equipment in situations where an initial search of the data uncovers some evidential material or where the officer believe on reasonable grounds that the equipment might contain evidential material."

This explanation inspired the Judge in *Kennedy v. Baker* to argue that data stored in the hard drive of a personal computer is a single thing regardless of whether it contains different parts, such as files and documents.

4.8.5 South African Legal responses to searching and seizing virtual evidence

South Africa is a democratic state based on the values of the supremacy of its Constitution and the rule of law (Constitution of the Republic of South Africa,1996). The basic

principles of criminal procedure have been constitutionalized in the Bill of Rights in the Constitution in the form of both general provisions, which are relevant to criminal procedure, and in the form of provisions which are specifically aimed at criminal justice (Neiman 2006:154). The Criminal Procedure and Evidence Act (31) was enacted after the establishment of the Union of South Africa in 1910. Many amendments followed. A consolidating Criminal Procedure Actl8 replaced it in 1955. This Act was repealed by the present Criminal Procedure Act, which came into force on 22 July 1977. In the South African legal context, the terms search and seizure are not clearly defined (Swanepoel 1997: 374). Basdeo (2009:310) assert that the question of what constitutes a search is left to common sense and is determined on a case by case basis. McQuiod (1977) substantiate that an element of physical intrusion concerning a person or property is necessary to establish a search .

According to Basdeo (2009:138), the Criminal Procedure Act (51 of 1977) has long been the primary statute under which the SAPS have the right to conduct searches and seizures in South Africa − with or without warrants. These rights are not left entirely to the discretion of the SAPS, but are subject to authorisation of authorised officers. Section 21 of the Criminal Procedure Act (51 of 1977) sanctions authorised officers to issue search and seizure warrants authorising police officers to enter premises and to search premises and persons on the premises to find and seize specific items on such premises − if there are reasonable grounds to believe that articles involved in the commission of a crime will be found on the premises. Section 21(3a) of the Criminal Procedure Act provides that a search warrant must be executed during the day,49unless the judicial officer who issues it gives written authorisation for it to be executed during the night. The reasonableness of the time when a warrant is executed is significant in terms of the Constitution, since it has an important effect on the extent to which the dignity and privacy of the person concerned is affected (Applied Law for Police Officials, 2002:310).

The Criminal Procedure Act 51 of 1977, section 21(3b) state that, a warrant may be issued and may be executed on a Sunday, as on any other day. It remains in force until it is acted upon or is cancelled by the person who issued it, or, if such person is not available, by a person with the same authority. Section 21(4) of the Criminal Procedure Act provide that

law enforcement officer executing the warrant under section 21 must, after such execution, upon demand of any person whose rights in respect of the search and seizure have been affected, hand a copy of the warrant to the person. These articles, which may be seized according to Section 20 of the Criminal Procedure Act 51 of 1977, are limited to articles, which is believed or on reasonable grounds believed to be (1) involved in the commission of a crime; (2) can be used as evidence; or (3) intended in the commission of a crime.

As was expressed in the case of *NDPP and Another v. Mohamed*, the search and seizure of articles from a premises is a significant invasion upon the rights of individuals and should be completed within clearly defined limits so as to impact as little as possible on the rights of affected individuals. Section 82(3) of the Electronic Communications and Transactions Act stipulates that the Criminal Procedure Act applies with the necessary changes to searches and seizures in terms of the Electronic Communications and Transactions Act.36 It is interesting to note that section 82(4) provides specifically that any reference in the Criminal Procedure Act to "premises" and "article", for the purposes of the Electronic Communications and Transactions Act, includes an information system, as well as data messages (Nieman 2009:159).

Concerning cybercrime search, Chapter XII of the Electronic Communications and Transaction Act provides for the appointment of cyber inspectors within the Department of Communications. Section 81(1) of the Electronic Communications and Transaction Act provides for the general powers68of cyber inspectors Section 80(4) of the Electronic Communications and Transactions Act. Section 80(2) of the said Act requires a cyber inspector to be provided with a certificate of appointment signed by or on behalf of the Director-General of the Department of Communications. The certificate must state that the cyber inspector has been appointed as such a cyber inspector.

Section 82 of the Electronic Communications and Transactions Act “provides that a person who refuses to cooperate or who hinders a person conducting a lawful search and seizure in terms of section 82 is guilty of an offence. It is interesting to note that, in addition to section 82, section 80(5)(a) also criminalises obstructing the course of justice in this context. It provides that any person who hinders or obstructs a cyber inspector in the

performance of her functions in terms of chapter XII of the Electronic Communications and Transactions Act (including section 82) is guilty of an offence. A person who falsely claims to be a cyber inspector is also guilty of an offence. The penalties attached to all three offences are a fine or imprisonment for a period not exceeding 12 months.

According to Cheadle, Davis and Haysom (2012:193), the safeguards against unjustified interference with the right to privacy include prior judicial authorisation and an objective standard, that is whether there are reasonable grounds to believe based on information under oath that an offence has been or is likely to be committed; that the articles sought or seized may provide evidence of the commission of the offence; and that the articles are likely to be on the premises to be searched In the *Minister for Safety and Security v. Van Der Merwe and Others* (2011) case, it was stated that search and seizure warrants govern the time, place and scope of intrusions or violations. Obtaining search and seizure warrants under the Criminal Procedure Act section 51 was identified by the court in the *Magajane v. the Chairperson of the North West Gambling Board* (2006) case as a tried and tested mechanism whereby courts can defend individuals against the power of the State and against unlawful searches. Search and seizure warrants issued in terms of the provisions stipulated in the Criminal Procedure Act section 51 important weapon that assists the SAPS in performing their constitutional mandate of preventing and investigating crime. However, by utilising this powerful tool, they interfere with the equally important rights of individuals. Safeguards are, therefore, needed to ameliorate the effect of these infringements by limiting the extent to which the rights of individuals are impaired. In the *Minister for Safety and Security v. Van Der Merwe and Others* (2011) case, the court stated that aggrieved suspects can question the validity of search and seizure warrants on the basis that these warrants were too vague – overbroad − that it extend beyond what is permitted 68 by the statute or is absent of jurisdictional facts that are foundational to issuing the search and seizure warrant.

4.9 COMPARATIVE LEGAL ANALYSIS

Marghaireh (2011:160) remarks that laws obligate law enforcement officers to draft a search warrant based on probable cause or reasonable grounds. The general rule is that all searches and seizures conducted without a warrant are unreasonable and violate

jurisdictional legislations (Ferdico *et al* 2015:271). Police officers must have probable cause as the threshold to justify the issue of a conventional search warrant (Marghaireh 2012:115). The Ghanaian criteria or the threshold set by the Criminal Procedure Code 1960 (Act 30) to issue a search warrant is simple and serve justice to investigators and law enforcement. If any one of the following four circumstances is applicable: first, a thing in respect of which an offence has been committed, Second, a thing which is intended to be used for the purpose of committing an offence, third, a thing which has been unlawfully obtained, and fourth a thing of which possession is unlawful. The search shall be done in daytime (6:30a.m and 6:30 p.m.) but can also be done at any other time if authorized by a Court. The tenant/ occupant, his representative or an adult tenant neighbour shall be summoned to attend the search. And as a general rule all searches should be conducted with the cooperation of the local Police under whose jurisdiction the arrest/search is going to be conducted. This is applicable to virtual search or cyber search warrant for law enforcement. In contrast, the United States, United Kingdom and Australia threshold in the issuance of search warrant is complex.

Hayes and Eburn (2016:612) observe that the reasonable belief of a prudent man is being used in both Australia and the USA to evaluate the reasonableness and legitimacy of the "probable cause" requirement for issuance of a search warrant. In addition Marghaireh (2013:200) assert that factual evidence linking criminal activity and the item to be seized, and between the place to be searched is an important for in drafting warrant and because reasonable belief of a probable belief of a prudent man is unfetted by a fixed parameter and varies with each case and officer's. Marghaireh (2013:177). The United States of America PATRIOT Act (32) is a statute enacted by the United States government in October 2001. The Act increases the ability of law enforcement agencies to search e-mail communications, telephone, medical, financial and other records and enhances the discretion of law enforcement agencies in detaining and deporting immigrants suspected of terrorism related acts. In the United States, the Supreme Court in 1971 made it clear that neither prosecutors nor police officers can be asked to maintain the requisite neutrality when deciding whether a search warrant should be issued (*Coolidge v New Hampshire 403 U.S. 433 [1971]).* State courts have recited the rule in state decisions. For example, an Oklahoma court held that the purpose of the warrant is to allow a neutral

judicial officer to assess whether the police have probable cause to make an arrest or conduct a search *(Mollet v State 939 P.2d 1 [Okla.1997] 743).*

Marghaireh (2013:187) asserts that applying the traditional procedures of knocking and notifying to the place the search may jeopardise the integrity of the evidence that is going to be discovered because digital evidence can be quickly and easily destroyed even by something as simple as pressing a hotkey Law enforcement can always be successful in searching and seizing evidence when they used sneak tactics or take the suspect by surprise to avoid destruction of evidence. Therefore using sneak and peck search warrant, instead of a traditional or classical search warrant that involve knocking and notifying is welcome and self-evident in digital search and seizure and digital investigation than any other investigation.

In South Africa, section 25(1) of the Criminal Procedure Act provides that if it appears to a magistrate or justice from information on oath that there are reasonable grounds for believing: that the internal security of the Republic or the maintenance of law and order is likely to be endangered by or in consequence of any meeting which is being held or is to be held in or upon any premises within his or her area of jurisdiction; or (b) that an offence has been or is likely to be committed or that preparations or arrangements for the commission of any offence are being or are likely to be made in or upon any premises within his area of jurisdiction. In *Control Magistrate, Durban v AZAPO,29* warrants were issued in terms of section 25(1) of the Criminal Procedure Act, on the basis of confidential information supplied to the magistrate in affidavits. The magistrate failed to provide reasons for his belief that the circumstances mentioned in section 25(1) existed (Basdeo, 2009:66). On appeal the decision by the provincial division setting the warrants aside was reversed. Only information placed under oath before a magistrate or justice may be considered in coming to the decision to issue the warrant (*Naidoo and Another v Minister of Law and Order and Another 1990 (2) SA 158 (W) 166*.). “In *Wolpe v Officer Commanding South African Police*, Johannesburg thirty one (31) police officials entered a hall where a conference was being held by the South African Congress of Democrats together with other organizations (Basdeo, 2009:66). The chairman requested the police to leave the meeting and indicated that it was a private meeting but the police refused to

leave. The Congress of Democrats brought an urgent application to the court for an interdict to prohibit the police from attending the meeting. They argued that the police do not have greater powers than any other individual, except in so far as they are vested with wide powers by statute. The application was refused. The judge concluded that if there was a suspicion that as a result of the holding of the meeting a disturbance of public order would occur on the same day, the police were entitled to attend the meeting in order to prevent the disturbance of order, even though the meeting was private (Basdeo, 2009:66). Furthermore in South Africa As a general rule a search should be authorised by a judicial officer (Sections 21(1) and 25 of the Criminal Procedure Act). This power is, however extended to justices of the peace (Section 21 of the Criminal Procedure Act).Where the person issuing the warrant is part of the office of the executing officer, then objectively, there is no neutral or detached officer.

4.10 PRIVACY PROTECTION IN SEARCHING AND SEIZING DIGITAL EVIDENCE

In criminal case, for the law or legislation to be applicable to a particular fact situation, there must be a seizure or a search and seizure accompanied by an attempt by the prosecution to introduce what was seized as evidence in court. Whether there was a search or seizure within the meaning of the law and if so, whether the search or seizure violated someone's constitutional rights depends on the nature of the interest that the law protects. Ferdico (2015:106) assert that under the common law, it was clear that the security of one's property was a sacred right and that protection of that right was a primary purpose of government. In the United States, the protection of property interests as the basis of the fourth Amendment was adopted by the U.S. Supreme Court, and until relatively recently, analysis of Fourth Amendment issues centered on whether an intrusion into a constitutionally protected area had occurred. In *Olmestead v. United States,* 277 U.S. 438 (1928), one reason for the Court's holding that wiretapping was not covered by the Fourth Amendment was that there had been no physical invasion of the defendant's premises. The Court said: the evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched. Furthermore, in *silverman v. United States,* 365 U.S. 505

(1961), however, a spike mike was pushed through a common wall until it hit a heating duct, and the Court held that the electronic surveillance was an illegal search and seizure. And in *Clinton v. Virginia, 377 U.S. 158 (1964),* the Court ruled inadmissible evidence obtained by means of mechanical listening device stuck into the wall of an apartment adjoining the defendant's. In *Katz v. United States,* 389 U.S. 347 (1967), another electronic surveillance case, dispensed with the requirement of an actual physical trespass in applying privacy the United States Fourth Amendment. The court held that the government's electronically listening to and recording the defendant's words violated the privacy on which the defendant justifiably relied when using the telephone booth and thus constituted a search and seizure within the meaning of the Fourth Amendment. The added, "The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance. The katz case signaled a major shift in the interpretation of the Fourth Amendment away from a property approach toward a privacy approach.

4.11 CHAPTER SUMMARY

When conducting a crime search and investigation, the investigator first needs to establish the legal authority to perform a search. Once at the crime scene, the boundaries of the scene need to be established, along with a single point of entry and exist. All nonessential personnel should be removed from the crime scene. Once the crime scene is secure, the investigators must identify potential evidence and determine which evidence can be lawfully collected from the crime scene. Both the crime scene and the evidence to be seized should be thoroughly documented. Following the documentation of the evidence, an investigator must label, package, and transport the evidence to a forensic lab. At the lab, the items must be inventoried, recorded, and secured in a climate-controlled environment. If there is a problem with how the evidence was collected, handled, or processed, the evidence may be rendered inadmissible in court. To make

sure the evidence is considered admissible in court, the proper retrieval, identification, analysis, and preservation of evidence is required.

CHAPTER FIVE

DIGITAL EVIDENCE ADMISSIBILITY AND EVIDENTIAL WEIGHT IN THE COURTROOM

5.1 INTRODUCTION

Computer systems may crash. Files may be accidentally deleted. Disks may accidentally be reformatted. Computer viruses may corrupt files. Files may be accidentally overwritten. Disgruntled employees may try to destroy your files. All of these can lead to the loss of your critical data. The escalation of cybercrime and other network-related serious crime has made digital evidence increasingly important. “Electronic evidence and information gathering have become central issues in an increasing number of conflicts and crimes. Digital evidence can reveal the signature behaviour of cyber criminals, such as malware developers and hackers (Casey, 2011:230). Signature *behaviour* is a recognizable and distinguishable pattern of activity (e.g., specific techniques, tools, and monitoring) that can be attributed to a source, which provides some form of psychological or emotional benefit (e.g., gratification and recognition by peers) to the cybercriminal (Casey, 2011:231).

Antwi (2018:42) posit that, digital evidence has become considerably important because of the involvement of the internet and electronic devices in criminal activities. Casey (2019:201), Kerr (2013a, 2013b), and others have observed that digital evidence is growing in both volume and importance in criminal and civil litigation. Judges must decide what evidence will be admitted in their courtroom and need to weigh the probative value against the prejudicial effect of any evidence that is offered (Cohen, 2010). These considerations apply to scientific and technical evidence as well as to other types of physical evidence such as crime scene photographs, shell casings, and blood splatter diagrams. To fairly and justly evaluate the merit of digital evidence, judges should have some understanding of the underlying technologies and applications from which digital evidence is derived, such as computers, the Internet, and e-mail. As technology continues to develop in scope and relevance, so does the need to rely on digital evidence in the administration of justice, be it criminal, civil or corporate-level investigations (Antwi, 2018:42). Leigland and Krings (2004) claim that riding on the tide of the current Information and Communication Technology (ICT) revolution, criminals have expectedly transitioned to the use of computers, mobile devices and other digital channels to commit crimes. Antwi (2018:42) reveals that this development requires criminal justice actors to investigate, produce and present evidence through a process that is legally admissible and capable of securing successful prosecution.

5.2 THE CONCEPT OF DIGITAL EVIDENCE

Andre (2018:153) state that central to any digital investigation is the notion of digital evidence. Digital evidence is defined as any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi (Chisum 2011:120). According to Kessler (2011:96), digital evidence is simply a product of digital forensics. Reveals done by ISO/IEC 27037 defined digital evidence as information or data stored or transmitted in binary form that may be relied upon as evidence. Cohen (2010:86) agrees with the above narrative and further describes digital evidence as the product of a digital forensics process. The Council of Europe (COE) defines digital evidence as "any information generated stored or transmitted in digital form that may later be needed to prove or

disprove a fact disputed in legal proceedings" (Council of Europe Convention on Cybercrime 2013).

Casey (2011:224) claims that digital evidence is any data that can establish that a crime has been committed or can provide a link between a crime and its victim or a crime and its perpetrators. A broader definition proposed by the Association of Chief Police Officers (2012) is information and data of investigative value that are stored on or transmitted by a computer. Digital evidence begins as electronic data, either in the form of a transaction, a document, or some type of media such as an audio or video recording. Transactions include financial transactions created during the process of making a purchase, paying a bill, withdrawing cash and even writing a check. While writing a check might seem to be an old–fashioned method that is not digital or electronic in nature, the processing of that written check is electronic and is stored at your bank or credit card company. Nearly every kind of transaction today is eventually digitized at some point and becomes digital evidence. Doctor visits, construction projects, getting prescriptions filled, registering a child at daycare, and even taking the pet in for a rabies shot.

Larry and Lars (2012:56) assert that in today's connected world, it is nearly impossible to be completely "off the net" such that your activities do not create some form of an electronic record. The explosion of social media sites has created a whole new area of electronic evidence that is both pervasive and persistent. People today are sharing their everyday activities, their thoughts, their photos, and even their location via social media such as Twitter, Facebook, MySpace, and blogsphere, where individuals act as citizen journalists and self–publish blog posts on the Internet ranging from their political views to their family blogs with pictures of their kids and pets. Terrorists are using the Internet to communicate, recruit, launder money, commit credit card theft, solicit donations, and post propaganda and training materials. Computers played a role in the planning and subsequent investigations of both World Trade Center Bombings. Ramsey Yousef's laptop contained plans for the first bombing and, during the investigation into Zacarias Moussaoui's role in the second attack over 100 hard drives were examined (United States v. Moussaoui.; United States v. Salameh *et al*.; United States v. Ramsey Yousef). Network-based attacks targeting critical infrastructure such as government, power health,

communications, financial and emergency response services are becoming a greater concern as state-sponsored groups have become more technologically proficient.

Larry and Lars (2012:78) assert that there is a positive aspect to the increasing use of technology by criminals and involvement of computers in crime has resulted in an abundance of digital evidence that can be used to apprehend and prosecute offenders. For instance, digital traces left on a floppy diskette that was sent by the Bind Torture Kill (BTK) serial Killer to a television station led investigators to a computer in the church where the serial killer Dennis Lynn Rader was council president.

Digital data are all around us and should be collected routinely in any investigation (Casey, 2012:123). Therefore, every corporate investigation should consider relevant information stored on computer systems used by their employees or criminals both at work and at home. Every search warrant should include digital evidence to avoid the need for a second warrant and the associated lost opportunities. Even if digital data do not provide a link between a crime and its victim or a crime and its perpetrators, they can be useful in an investigation. Digital evidence can reveal how a crime was committed, provide investigative leads, disprove or support witness statements, and identify likely suspects (Casey 2011).

5.2.1 Direct and Circumstantial Evidence

Evidence is used to prove either facts in issue, or facts from which facts in issue may properly be inferred' or any type of material left at, or taken from a crime scene, or the result of contact between two surfaces. Evidence can usually be measured, photographed, analysed and presented in court as a physical object and is ordinarily defined as the means of establishing and proving the truth or untruth of any fact that is alleged. Evidence can be the testimony of witnesses, physical objects, documents, records, fingerprints, photographs, and confirms that evidence, in the legal sense, includes only what is introduced at the trial and that the key to evidence is that it must be presented; if it has not been presented during the trial then it cannot be classified as evidence yet. Gardner and Anderson (2015:54) join the discussion by stating that evidence is ordinarily defined as the means of establishing and providing the truth or

untruth of any fact that is alleged. The authors quote the famous English lawyer and writer Sir William Blackstone's definition of evidence as “that which demonstrates, makes clear or ascertains the truth of the very fact or point in issue, either on the one side or other”.

According to Gardner and Anderson (2015:80), direct evidence is the evidence that proves or disproves a fact in question with no need for inferences. For example, a witness, Augustine testifies under oath that he saw Bernard wrote and sent a harassing message to his ex-wife. Further questioning shows that the witness has good eyesight, the witness was close enough to observe the incident, the lighting was good, and the witness both accurately described the defendant to the police and in the courtroom identified the defendant without any doubt. This is an example of strong, direct, credible evidence that would be sufficient to convict unless the defence could produce evidence sufficient to impeach the credibility of the witness. Another scenario: Augustina sits at his company’s laptop, enters her username and password, when and logs on to the system. She hacks into the company’s database and deletes certain files. When she is finished, Mary logs off her laptop and leaves the office. The day, the systems administrator notices that someone has deleted certain files from the company’s database. IT personnel are able to determine that Augustina’s laptop, username, and password were used in the incident. The direct evidence in this case is that Augustina laptop, username, and password were used to log to on to the system and delete the files.. Direct evidence is based on personal knowledge or observation of the person testifying. It is evidence that proves or disproves a disputed fact directly and relies on the senses and perception of the eyewitness and does not require any intervening or indirect fact to be proven first. If the testimony is believed, the fact it relates to is conclusively established.

Marras (2015:41) posit that circumstantial evidence allows someone to infer the truth of a given fact. Example is when a fingerprint is found on a laptop computer at the scene of crime. This fingerprint belongs to the suspect in the crime, John. This fingerprint is both direct evidence that John was at the scene of the crime and indirect (circumstantial) evidence that John committed the crime at the scene. Gardner and Anderson (2016:80) further state that circumstantial evidence is evidence that indirectly proves a fact in issue.

For instance, testimony that the defendant was at the scene of the crime and ran from the with a pistol in his or her hand is circumstantial or indirect evidence (Gardner and Anderson 2016:80). Circumstantial evidence proves or disproves a fact indirectly by first proving another fact, from which an inference may be drawn as to the original disputed fact. It requires the trier of fact to use an inference or presumption to conclude that the fact does exist, e.g. a witness placing the accused on the scene with no other possible suspect present or physical evidence, which in itself does not prove or disprove the guilt of the perpetrator. However, unless the existence, character or circumstance of the generation or storage of an electronic record is itself a fact in issue (Gardner and Anderson 2016:80), it is more frequently the case that electronic evidence is used as indirect evidence to prove certain facts from which the facts in issue may be inferred. For instance, if an electronic record is adduced in evidence to show that A owes B a debt, the electronic record as indirect evidence only proves that there is a record that A owes B a debt, and it is necessary to make the additional inference that A actually owes B a debt. Mason (2012) state that the circumstantial evidence can be used to authenticate an electronic document and such circumstantial evidence includes a range of factors including, but not limited to, appearance and the contents of the document, the subject matter, witness testimony, and any distinctive features that indicate a nexus.

5.3 LOCATION OF DIGITAL EVIDENCE

Marras (2015:199) indicate that digital evidence is most commonly found on hard drives. Data in the hard drives of computers consist of volatile and non-volatile data. The volatile data disappear when the computer is powered off, whereas nonvolatile data are stored and persevered in the hard drive when the computer is powered off. Digital evidence in the hard drives of computers may be found in files created by the computer user such as emails, spreadsheets, and calendars. Files protected by the computer user such as encrypted and password-protected files and files created by the computer such as log files, hidden files, backup files, and other data areas such as metadata.

5.3.1 Deleted Data

Data recovery is one of the foundations of digital forensics. Recovering files or data from hard drives and other media that have been deleted is part and parcel of a forensic examination. Evidence can be found and typically recovered by the investigator in files deleted by the computer user. However, the competency to recover deleted files in their entirety or at least the artefact that existed depends on the forensic application robustness.

- Figure 5.1 Deleted Data into recycle bin. Source EDUCBA.

When an operating system deletes a file it does not remove the data but it only changes the pointer to the file to tell the file system that the file no longer exists and the space is available for new data. “For this reason, in the vast majority of cases, it is possible to recover data that have been deleted, depending on the amount of disk writing activity that has been performed between the deletion of the file and the forensic analysis (Jones and Meyler 2014:183). This is illustrated by the case of *Sectrack NV v. Satamatics Ltd* (2007), concerning the misuse of confidential information. One of the defendants was in possession of a Blackberry device, which he claimed was frozen or locked. When the device was 'unlocked', it automatically downloaded various emails that the defendant

received, which implicated him in the misuse of confidential information. In this case, manufacturers of handheld devices have developed extensive backup systems that permit the backup of device data to other devices and storage facilities. In future, without the use of encryption, it will be relatively difficult to delete data sufficiently for it to be beyond recovery. Deleted files may affect suspect's culpability and enhance them to demonstrate criminal activities and hide their wilful actions. Marras (2015:150) further add that depending on which Windows operating system the investigator is dealing with, the file allocation table can be in the FAT, FAT32, or NTFS format. The FAT and FAT32 file allocation table are used in Windows 3.1, 95, 98, and ME edition and the NTFS are used in Windows NT, 2000, XP, 2003, 2008, Vista and Windows 7."

5.3.2 E-Mail Evidence

E-mail is probably one of the most prolific forms of evidence available today. It seems that everyone has an e-mail account, from children to octogenarians. E-mail or electronic mail has transcended social boundaries and moved from a convenient way to communicate to a corporate requirement in many businesses. Even so, users are typically more relaxed and unguarded using e-mail than they are when creating more formal written communications such as memos or letters sent by postal services. This psychological attribute has provided some interesting and, in many cases, incriminating unintentional documentation of people's activities or attitudes that can be found through digital evidence collection. In many cases, e-mail data can be pivotal evidence. Because of its informal nature, it does not always represent an "official" posture of an organization. However, in litigation matters such as sexual harassment cases, it does carry the onus of corporate policy.

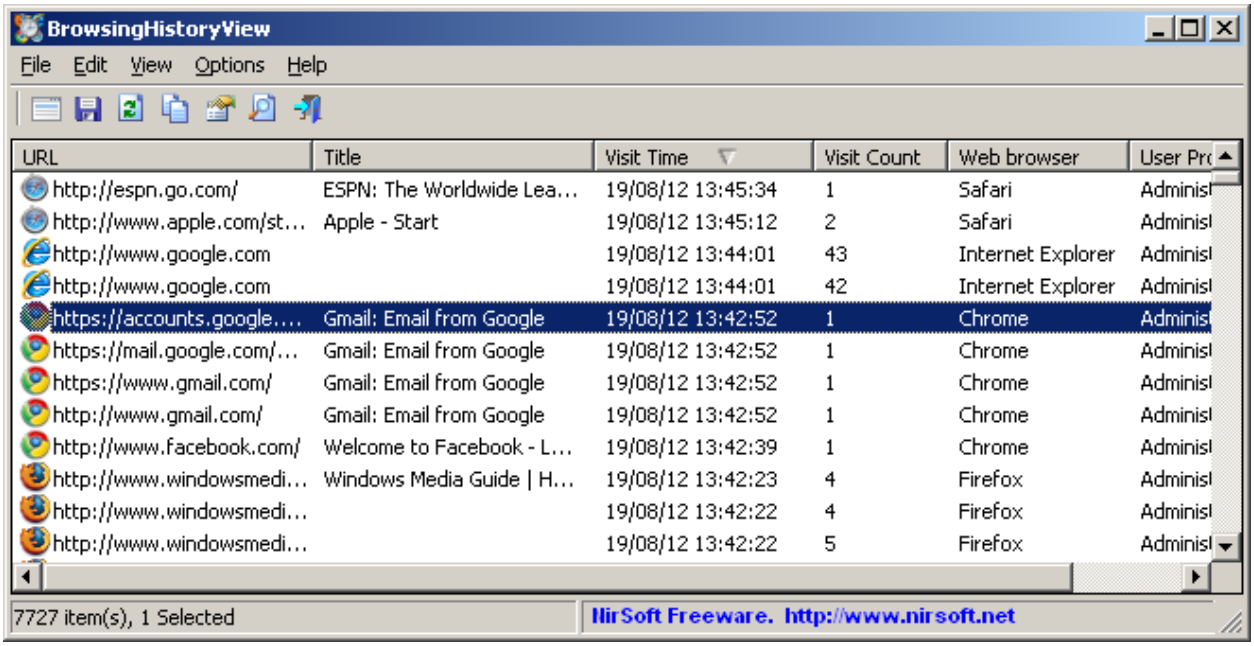
In the case of *Knox v. States of Indiana* 93 F.3d 1327 (1996), e-mail messages in which a supervisor repeatedly asked an employee for personal favours served as key evidence in a sexual harassment suit. Also, in the case of *Nardinelli et al v. Chevron* 467 U.S. 837 (1984) four employees filed suit against the firm claiming that they were sexually

harassed. To show that Chevron's management allowed a hostile work environment, emails containing jokes such as "twenty-five reasons beer is better than woman" were introduced into evidence. Chevron settled for $2.2 million plus legal fees and court costs. The forensic extraction and analysis of email continue to play a critical role in civil and criminal cases and may be used by either prosecution or the defence. E-mail evidence is typically used to corroborate or refute other testimony or evidence or to help guide an investigation. An example of the use of e-mail evidence to support other evidence occurred in the 2005 case of *State of North Carolina v. Robert J. Petrick,* COA7-86 (2007) who was on trial in North Carolina for Killing his wife Janine Sutphin. Petrick left a trail of digital evidence or E-evidence including e-mail messages and a visit to the Web site bloodfest666. Digital evidence or E-evidence included an e-mail Patrick sent to women he was having affairs with and the downloaded document "22 ways to kill a man with your bare hands" from his hard drive was found and presented to the court. Investigators also retrieved e-mails that Patrick's wife had sent before her death. According to the prosecutors, Robert Petrick did a Google search for the topics "neck snap break" and "hold" before she was killed. Investigators also claimed that before reporting his wife missing Petrick looked up the depth and topography of a lake where his wife's body was found. In general, e-mail is used by either side to influence alimony payments in a divorce case and to prove harassment or discrimination in employment cases.

5.3.3 Metadata

Metadata can be a veritable gold mine of useful information in a case (Larry & Lars 2012:179). Vahey (2012:110) recommends that metadata provide vital information about the history of the files since their creation to date because it describes how, when, and by whom the files were collected, created, accessed, or modified and how it is formatted, and thus all the information needed to identify and certify the scope, authenticity, and integrity of active or archival data. The prefix *meta* in English is used to express the idea that some information is about its category. Hence the meaning of metadata is "data about data". Metadata is not hard to understand in principle but can be confusing in detail. The purpose of metadata is to store information about other data. This can help with the organization and retrieval of data. For instance, web pages on the Internet have metadata

in such forms as meta-tags. A meta-tag is coded into a website where you do not see it, but it contains information about a website, such as keywords so that it can be easily found when those keywords match your Google search. Metadata can also be found inside many pictures and videos, containing copyright information if there is any, as well as information such as when the picture was taken and the make and model of the camera the picture was taken with. Below is a typical browsing history view. Figure 5.2 dipict an example of browser metadata extract from internet history.



- Figure 5.2 An example of browser metadata extracted from Internet history. Source: NirSoft Freeware.

The figure above shows browser metadata. The history stored by Internet browsing programs certainly qualified as data about websites and pages that have been visited, and websites or pages marked as favourites by the user. Browser metadata is used extensively as forensic evidence in all kinds of cases. Mason *et al* (2021:19) point out that all documents in electronic format will contain metadata in one form or another, including email communications, spreadsheets, websites and word processing documents. An electronic document has to have metadata to help interpret the purpose of the digital document. Such data can include, and be taken automatically from the

originating application software, or supplied by the person who created the record (Deng and Mason 2016:119).

The list of information that is available includes, but is not limited to: when and how a document was created (purported time and date), the file type, the name of the purported author (although this will not necessarily be reliable), the location from which the file was opened or where it was stored, when the file was last opened (purported time and date) when it was last modified when the file was last saved when it was last printed, the identity of the purported previous authors, the location of the file on each occasion it was stored, the details of who else may be able to obtain access to it, and, in the case of email, blind carbon copy (bcc) addresses (Mason Deng, Murdoch & Schafer 2017:148).

- Figure 5.3 is a typical example of document metadata. Source: Larry and Lars (2012).

In *Crinion v IG Markets Ltd* [2013] EWCA Cir. 587, the judgment of the trial judge, HH Judge Simon Brown QC, was taken word-for-word from the closing submissions of Mr Chirnside's counsel for the claimant, written in a Word file. The trial judge adjusted the text, and the 'properties' file in the Word version of the judgment indicated that the 'author' was shown as 'SChirnside.

Also, the person originating a document may not use a new file, but begin the document by opening an old file, deleting the majority of the text, and then creating the genesis of the new text; further, the name of the author may not be accurate if somebody other than the purported author logged on to a computer or system using the name of the person, and there may be occasions that a person uses software on their computer that has been installed and registered in another name – although if the metadata is correct, it can directly lead to a killer that has murdered several people over a long period, as in the case of *The State of Kansas v Dennis L. Rader*, 05CR498 (2005), 18th Judicial District Court, Sedgwick County, Kansas. The defendant entered a plea of guilty before Waller J. on 27 June 2005." A further illustration of the importance of metadata is the case of "*Campaign Against Arms Trade v BAE Systems PLC* ([2007] EWHC 330 (QB). Mr Justice King granted Norwich Pharmacal relief to the Campaign Against Arms Trade (CAAT), against BAE Systems PLC (BAE). On 29 December 2006, a senior officer of CAAT, Ms Feltham, sent an email to the members of the CAAT steering committee using an internal email list (caatcommiteee@lists. riseup.net), a private list not open to the members of the public and comprising only the 12 members of the steering committee and seven members of CAAT's staff.

The email contained privileged legal advice that CAAT received from its solicitors. A copy of the email was somehow sent to BAE. By a letter dated 9 January 2007 and received the next day, solicitors for BAE returned a copy of the email printed on paper to CAAT's solicitors. This was the first time that CAAT came to know of the leak. The printed email returned to CAAT was incomplete (because the email metadata was missing). As described by Mr Justice King: It was a redacted version of that which had come into the possession of the Respondent and/or its solicitors. All the routing information, the header address and so forth, which would give details of the email accounts through which the email had been received and sent before arriving at the Respondent and its solicitors, had been removed. Such removal must have been done either by the Respondent or by its solicitors acting on its instructions [2007] EWHC 330 (QB), [31].

A case from the United States of America serves to highlight how concerns relating to the preservation of data are viewed, and the relevance of metadata. In the case of *Armstrong v. Executive Office of the President, Office of Administration* F3d 1274, 1290 D.C. (Cir. 1993), researchers and non-profit organizations challenged the proposed destruction of federal records. The Executive Office of the President, the Office of Administration, the National Security Council, the White House Communications Agency, and the Acting Archivist of the United States intended to require all federal employees to print out their electronic communications on to paper to discharge their obligations under the provisions of the Federal Records Act. The members of the United States Court of Appeals, District of Columbia Circuit, rejected this solution, because, in the words of Mikva CJ, the hard copy printed version 'may omit fundamental pieces of information which are an integral part of the original electronic records, such as the identity of the sender and/or recipient and the time of receipt' (1 F.3d 1274, 1277 (D.C. Cir).

5.3.4 Computer Time Artefacts (MAC Times)

Undoubtedly one of the most important forms of digital evidence is computer time artefacts. These artefacts are mostly most commonly called MAC times, which stand for Modified, Accessed, and Created (Larry & Lars 2012:207).. Computer time artefacts play a critical role when achieving permanent acceptance of a timeline for a body of evidence for any case where time is of great significance or value. Larry and Lars (2012:129) argue that if the case involves an alibi, computer time artefacts can be used as part of a body of evidence to negate or validate the alibi claims. Computer time artefacts can be used to establish exactly when the alleged data theft occurred. However, some file systems record four dates including the additional last written date. Email time stamps can also be confusing unless you are careful in the interpretation of the method of recording the time and the correct time zone of the timestamp record (Larry & Lars 2012:207).

Timestamps provide valuable information to aid the investigation. This was demonstrated in *Jackson v. Microsoft Corporation*, where the timestamp data on confidential files in the

defendant's possession provided evidence of intellectual property theft. Timestamps have proven to be an expedient source of evidence for examiners in the reconstruction of computer crimes (Palmbach &Breitinger 2020).

5.3.5 Hash Values: The Verification Standards

As noted by Tipton and Micki (2017:197), "Hash value commonly known as hash algorithm or one-way function, on the other hand, works like a fingerprint image to authenticate the mirror copy and to determine whether the evidence contained in the copy has been the subject of any improper alteration." According to Xiaoyun, Wang and Hongbo (2015:19) hash value is a short string of random-looking letters and numbers generated by using an algorithm called a hash function, which is a mathematical formula used to encrypt and decrypt information, inserted into the original electronic documents when they are created to provide them with distinctive characteristics that will prove how they are created to provide them with distinctive characteristics that will prove their authentication. Antwi (2018:196) also state that hash is a mathematical function that converts a piece or a set of digital data into a constant numeral representation, usually used in digital forensics to ensure the integrity of digital evidence.

Larry and Lars (2012:67) maintain that Hash values play important roles in forensics, especially in verifying that a forensic image of digital evidence is the same as the original. Larry and Lars (2012:215) further add that in any court of law or when asked on the witness stand, any examiner should be able to show that he or she took the proper steps to verify the evidence collected using hash values for verification of the forensic copy against the original evidence. Ignoring the benefit of using hash values in a case beyond simply verifying evidence does them a great disservice (Larry & Lars 2012:216). Thomas (2011) advocates that hash uses every bit of a file to compute a unique result for the file, and hash results for a file can be used to see whether any bits in the file have changed. This is useful for the investigator to identify files and to demonstrate that a file has or has not changed. Proving a piece of digital evidence is performed by testimony which consistently identifies a particular piece of digital evidence and then set up on a firm or

permanent basis of a chain of custody, the location of the evidence at all times since its copying. The latent and voluminous nature of digital evidence makes discriminating differences between two pieces of data in practice infeasible without tools. As such, identification of digital evidence is achieved primarily through using hashing to generate a unique and more easily distinguishable individuate.

Larry and Lars (2012:211) indicated that when a hard drive is hashed for verification purposes, the hashing process looks at all of the data on the hard drive and creates a digital thumbprint for it. Message-Digest 5 (MD5) and Secure Hash Algorithm-1 (SHA-1) are the two common hash algorithms that are employed in digital forensics mainly for evidence integrity. Lacking to follow the fundamental steps of maintaining a chain of custody for evidence by creating a verification hash of collected evidence leaves the question of the authenticity of the evidence open. Larry and Lars (2012:205) argue that it is very common, especially in civil and domestic cases, to collect evidence as a point-in-time snapshot and posited that creating a verification hash of the collected is a vital step in ensuring that the collected evidence matches the original evidence at the time it is collected. Casey (2011:428) demonstrates that forensic investigators must take extreme care when creating the mirror copy and must calculate the hash value code of the original disk to clearly show that the mirror copy and the original version are identical. Hence, the claimant by a defendant that the mirror image created by the forensic investigators has made unauthorised alterations, forensic investigators can use the hash value to demonstrate the truth that the original data and the mirror copy are identical and no changes happened, because they have the same hash value.

The National Institute of Standards and Technology (NIST) has established certain requirements for computer forensics imaging tools. Once an exact copy of a suspect's hard drive has been made, the investigator must verify that it is an exact copy.

An investigator verifies this by computing an MD5 hash algorithm for both the original hard drive and the copy of the original drive. Hashing using the MD5 or SHA hash algorithm has a standard of certainty even higher than that of DNA evidence (Marie, 2015:220). Surprisingly, it has been checked or proved the validity by courts. For

example, In *State v. Morris* , prosecutors not only validated the MD5 hash values process but also validated the forensic imaging process. Marras (2015:220) posit that the integrity of an investigation is ensured by imaging an exact copy of the hard drive or other media using the proper software. In *Gates Rubber Co v. Bando Chemical Industries Ltd (1996),* the court held that creating a mirror image copy of the hard drive is considered the most complete and accurate method for processing evidence. Also, in *Roads and Traffic Authority v. McNaughton*, the defendant's lawyer filed a motion to suppress digital evidence produced by a speed camera on the ground that the MD5 algorithm used to authenticate the evidence was weak. The Hornsby Court dismissed the charge because the Road Traffic Authority (RTA) failed to find an expert willing to testify that the photos had not been tampered with. By contrast, in Bursleon v. the United States, the court determined that the evidence was authentic because, among other things, the programme or the system which processed the documents was known to be trustworthy and reliable within the computer industry.

5.4 LEGAL ISSUES ON ADMISSIBILITY OF VIRTUAL EVIDENCE IN THE COURTROOM FROM THE COUNTRIES UNDER STUDY

In order to prosecute the virtual or cyber-criminal, a court requires sound digital or electronic evidence. If the integrity of the evidence presented in the court could not be proved then it becomes inadmissible. “If there is even a doubt that the evidence could have been tampered with then its integrity becomes questionable. If there is some period when the evidence could have been mishandled or it could have been in the custody of an unauthorized person, its integrity is doubted. From the time of collection of the evidence till the prosecution of the case, evidence integrity must be kept sound and its chain of custody must also be made tamperproof. Matti (1997:200) posits that the common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international co-operation, should be recognized. In many countries, such as the United States, United Kingdom, Australia and South Africa, different categories of digital evidence are regularly introduced to courts. The legislative body of some countries or states has been attempting to keep up with changes in

technology by continuously establishing new legal and authoritative acts or laws and revising existing laws.” Ghana's situation is similar, but not completely the same as the digital evidence usage, and prosecution of cybercrime is lower than in countries like the United States, United Kingdom, Australia and South Africa.

5.4.1 Ghana Legal Response to Admissibility of Digital Evidence

Admissibility of digital evidence in Ghana is found in various statutes such as the Electronic Transaction Act 772 of 2008, Evidence Act 323 of 1975, Criminal offences Act 29 of 1960, Cybersecurity Act 1038 of 2020, Criminal Procedure Act 30 of 1960, Anti-Money Laundering 749 of 2008. Athough these laws acknowledge all categories of digital evidence, each of these laws describes or defines a specific situation in which digital evidence might be admitted by judges at trial or in court.

The Electronic Transaction Act 772 of 2008 applies to transactions conducted over by electronic means and is considered as a special statute. This law addressed specific categories of digital evidence that courts may determine to admit in the courtroom. Electronic Transaction Act 772 of 2008, specify or set out electronic records, contracts, messages and signatures shall be deemed to produce the same legal effect as written documents. The Act provides specific rules by which courts should admit electronic evidence. Section 7 (1) of the Act highlight that, the admissibility of an electronic record shall not be denied as evidence in legal proceedings except as provided in this Act.

However, In assessing the evidential weight of an electronic record by judges in Ghanaian courtroom, section 7 (2) of the Act stipulate that the Court shall have regard to:

(a) the reliability of the manner in which the electronic record was generated, displayed, stored or communicated
(b) the reliability of the manner in which the integrity of the information was maintained,

(c) the manner in which its originator was identified, and
(d) any other facts that the Court may consider relevant.

Notwithstanding the fundamental rules of “relevancy” contained in the Evidence Act 323 0f 1975 are applicable in assessing the admissibility of any form of evidence including that which is electronic in nature. It is important to note that the general rules regarding admissibility of evidence cannot and are not replaced by the rules on admitting electronic evidence. The Electronic Transaction Act 772 of 2008 set in position what is considered digital evidence. The Act termed digital evidence or electronic evidence as electronic records such as contracts or messages generated through communication networks or messages sent, received, or stored by electronic means and any agreement by electronic means is termed as an electronic contract. At the same time, a digital signature or electronic signature is defined in the Act as any letters, characters, numbers or other symbols in digital form created or adopted by users of the communications networks systems to sign a document over the internet based –information and technological systems. The Evidence Act 1975 (N.R.C.D 323), Criminal Procedure Code (Act 30) which contains the existing rules for regulating methods of proof on physical evidence can be applied in restricted areas to digital evidence or electronic evidence. The Criminal offences Act 1960 (Act 29) did not address the admissibility of digital evidence but defined offences and punishments and gives the judiciary the power to evaluate and admit evidence on each according to the facts of the particular case.

Ghana has an adversarial system of criminal justice in which the offender is presumed innocent until proven guilty.

The Criminal Procedure Code 1960 (Act 30) provides judges with the power or right to summon and question experts to consent to the admission of evidence. Also, Section 67(1) of the Evidence Act 323 of 1975, states that a person is qualified to testify as an expert if, to the satisfaction of the Court, that person is an expert on the subject to which the testimony relates by reason of the special skill, experience or training of that person. Section 50 (1) of the Criminal Procedure Code 1960 (Act 30) empowers the judge to require any information for the purpose of detecting the commission of offences. Section

50 (2) of the same Act states that a person required by any such directions to furnish information shall also produce such books, accounts or other documents in his possession or control as may be required for the said purpose by the Attorney-General, or by the person authorised to require information, as the case may be (Criminal Procedure Act 30 of 1960). Furthermore, Section 53 (1) highlights the punishment for failure to disclose or give information and recommends that a person who fails to comply with any directions under section 50, whether with respect to the furnishing of information or the production of documents or who in furnishing any information in compliance with directions under section 50 makes any statement which he knows to be false in a material particular or recklessly makes a statement which is false in a material particular shall be guilty of a misdemeanour.

5.4.2 United States (US) Legal Response to Admissibility of Digital Evidence

In the United States, each state has the powers granted to them by the constitution. Each state has its criminal code, and each has enacted a code of criminal procedure and evidence. These codes and the rulings of the state courts must conform to the requirements of the U.S. Constitution. However, state laws and state court rulings may provide additional rights to the people of the state and criminal defendants within that state, beyond those extended by the Constitution.

The United States Congress Federal Rules of Evidence codification in 1975 of common law rules of evidence applicable only in federal courts but provides the model for most state evidence codes. The federal rules of evidence and most state rules of evidence apply in both civil and criminal trials. The majority of crimes committed in the United States are violations of state criminal codes. Some crimes are federal offences in violation of the federal criminal code. In any trial in the court of the United States, the Federal Rule of Evidence (FRE) provides guidance for determining sufficient grounds for admitting digital evidence. Rule 1001 explains evidence content as writing and recording that consist of letters, words, numbers, or their equivalent set down by handwriting, typewriting, mechanical or electronic recording or another form of data compilation. Before any digital

evidence is searched, seized and transported to the court, investigators must have at least a basic understanding of both the legal and relevant and technical issues pertaining to digital under the Federal Rules of Evidence. A critical rule is the Federal Rule of Evidence 1002, which is the best evidence rule. The best evidence rule of the Federal Rule of Evidence states that "to prove the content of a writing, recording, or photograph, the original writing, recording or photograph is required, except as otherwise provided in these rules or by Act of Congress." The term or words used in rules, such as "original writing" in Federal Rules of Evidence 1002, are sometimes explained in some other rule. To explain what is legally considered to be "original" writing or recording, Federal Rules of Evidence states that " if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an “original.”

When combined, Federal Rules of Evidence 1001 and 1002 mean that paper printouts of electronic materials qualify as originals as long as they are accurate. These rules are important to computer forensics investigators because they mean that there is no need to drag computer equipment into a courtroom simply to admit digital documents or e-mail messages into evidence (Federal Guidelines for Searching and Seizing Computers, 1994). The Federal Rules of Evidence 1003 allow the court to admit a mirror copy of the same evidence, and Rules 901 provide demonstration or exemplification of evidence authentication. In the case of the *United States v. Salcido*, 506 F.3d 729, 733 (2007) data from the defendant's computer was properly introduced under Rule 901. In the case of *United States v. Meienberg,* 263 F.3d 1177, 1181 (10th Cir. 2001) the district court correctly found that sufficient evidence existed under Rule 901. The proponent need not prove beyond all doubt that the evidence is authentic and has not been altered (*United States v. Gagliardi*, 506 F.3d 14 15 [2007]). An expert witness can be summoned by the court to testify that the digital data or applications and programmes which are used to process and produce such evidence are dependable and the status of presented evidence is the same as when it was collected. In the case of *United States v. Gagliardi,* 506 F.3d 140, 15 (2007), the court allow the witness and undercover agent to sufficiently authenticated emails and chat log exhibits by testifying that the exhibits were accurate records of communications they had had with the defendant. Also in the case of *United States v. Kassimu* 05-31087 (5th Cir. 2006), the district court correctly found that

computer records were authenticated based on the Postal Inspector's description of the procedure employed to generate the records. Authentication requirements are "threshold preliminary standards to test the reliability of the evidence, subject to later review by an opponent's cross-examination. *Lorraine v. Markel American Ins. Co*., (241 F.R.D. 534, 544) (citing *Jack B. Weinstein with Margaret A. Berger*, Weinstein's Federal Evidence § 900.06

Even though many courts in the states have categorically determined that computer records are admissible under Federal Rule of Evidence 803(6), increasingly, however, courts have recognized that many computer records result from a process and are not statements of person and they are thus not hearsay at all. In *United States v. Washington,* 498 F.3d 225, 230-31 (2007), the judge stated that the printed result of a computer-based test was not the statement of a person and thus would not be excluded as hearsay. Also, in the case of *United States v. Hamilton,* 413 F.3d 1138, 1142-43 (10th Cir. 2005)) the judge claimed that computer-generated header information was not hearsay as "there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801"; and in the case of *United States v. Khorozian,* 333 F.3d 498, 506 (3d Cir. 2003) "nothing 'said' by a machine is hearsay.

5.4.3 United Kingdom (UK) Legal Response to Admissibility of Digital Evidence

Despite the judicial statement of concern, the United Kingdom's (UK) responses on the admissibility of digital evidence or electronic evidence are recognized at both civil and criminal trials. The United Kingdom Civil Evidence Act (1995) was enacted to make available use for electronic evidence admissibility at the court of law, and also make adequate preparation for proof of certain evidence that is documentary and official actuarial tables in civil proceedings. Section 3 of the Civil Evidence Act makes computer records admissible in the United Kingdom courts. By merit of section 8 of the Civil Evidence Act, proof of statements in documents may be made by the production of such document or a copy thereof before the court. In that spirit, such documents include plans, photographs and models in accordance with Rule 33.6 of Part 33 of Miscellaneous Rules

about Evidence of the Civil Evidence Act 1995. At the same time, the United Kingdom Police and Criminal Evidence Act 1984 defined electronic evidence as 'all information contained in a computer and therefore admissible as evidence in the courts of law. In the case of *Castle v. Cross* (1 WLR 1372. [1984]), the prosecution sought to rely on a printout from a computerised breath-testing device and the Court held that the printout was admissible evidence.

Pursuant to the above case, further clarification was sort in the leading case of *R v. Shephard* (1988) 86 Cr App R 47. In this case, records from till rolls linked to a central computer in a shop were produced to prove that items in possession of the accused had not been billed and had thus been stolen by the accused and the court further held that so long as it could be shown that the computer was functioning properly and was not misused, a computer record can be admitted as evidence. The same principle was applied in *R v. Spiby* (1991) Crim. L.R. 199 (C.A.Cr.D.), the Court of Appeal held that printouts from an automatic telephone call logging computer installed in a hotel were admissible as they constituted real evidence.

The Court concluded that in the absence of evidence to the contrary, the machine had been in working order at the material time. Also, in the case of *Camden London Borough Council v. Hobson [1992],* "it was stated that computer-generated evidence constituted real evidence if the statement originated in the computer. It would then be admissible as the record of a mechanical operation in which human information had played no part; however, a statement originating from a human mind and subsequently processed by a computer would be inadmissible as hearsay. Considering the case of *Intercity Telecom Limited with Anor v. Sanjay Solanki (*LR 315, 2015) the court was satisfied that the evidence in the forms of a laptop, iPad and three universal serial bus (USB) pen drives which contained confidential information belonging to the company was admissible as evidence in the court of law." Similarly, in the case of *Atkins v The Lord Chancellor* (EWHC 1387. 2014), part of the evidence used in the proceeding was closed circuit television (CCTV) system and footage captured at the railway station showing what, how

and when things took place at the railway station. The court admitted the CCTV system and footage for the purpose of the proceeding.

In income tax assessment case between *Glenn Whittle v The Commissioner for Her Majesty's Revenue with Customs* (UKFTT 254. 2014), the evidence gathered and tendered during prosecution was in the forms of computer printouts of the appellant's bank account statement, taxi fare metered records and other computerised records kept and saved by the appellant for the purpose of preparing tax returns. All these computerised documents were tendered as evidence and admitted by the court as computerised evidence. On this note, it is provided that a video recording may be admitted as evidence in chief, specifically, if the evidence was taken from vulnerable witnesses, such as pursuant to Youth Justice and Criminal Evidence Act 1999. Where a video recording is to be adduced during proceedings before the Court, it should be produced and proved by the interviewer, or any other person present in the interview with the witness during which the recording was made, as required pursuant to Paragraph 27B.3 of the Practice Criminal Directions 2013. Audio and video 125 recorded interviews may also be admitted as evidence pursuant to Para 27C of the same Directions.

5.4.4 Australia Legal Response to Admissibility of Digital Evidence

Ainslie and Littrich (2017:114) reveal that legislatures have responded positively to the growing importance of digital evidence and some courts such as the supreme Courts in New South Wales and Victoria have issued practice notes encouraging litigants and lawyers to use technology in civil litigation. The evidential law of Australia is mixture of common law and statutes that establish the rules concerning evidence admissibility and as a result there are distinctions in addressing digital evidence. Most courts apply the Commonwealth Evidence Act 1995 and the Uniform Evidence Act 1995 at the Federal level and other states level. The commonwealth Evidence Act is applied by courts in the Australian Capital Territory but the New South Wales (NSW) and Tasmania on the other hand use the Uniform Evidence Act. The Australian Law Reform Commission (2004) posit that these statutes are substantially the same, but not identical. However, concerning

digital evidence admissibility, they are identical. The Australian Evidence Act defines documents to include digital evidence or electronic evidence. The Act describes documents as any record of information including (b) anything on which there are marks, figures, symbols or perforations, having a meaning for persons qualified to interpret them; or (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else (Evidence Act, 1995). In some Australian territories or states such as Victoria, Queensland, and South Australia, the Evidence Act makes specification states that evidence derived from computers will be admissible, subject to certain conditions of reliability. For example, the South Australia Evidence Act (1929) Section 56 allows the court to admit Evidence produced by processes, machines and other devices. Section 56(1) of the South Australia Evidence Act serves as a primary section that deals with the admissibility of digital evidence and further adds that for digital evidence to be admissible in court it must be subject to the court being satisfied:

> (a) that is produced wholly or partly by a device or process; and
> (b) that is tendered by a party to proceedings who asserts that, in producing the document or thing, the device or process has produced a particular outcome.

The South Australia Evidence Act also enshrines powers to the court to admit documents that have been modified because Section 57 emphasises on modification of the best evidence rule. Section (57)1 states that A document that reproduces the contents of another document is admissible in evidence before a court in the same circumstances, and for the same purposes, as that other document (whether or not that other document still exists). This section applies to a reproduction made:

> (a) by an instantaneous process; or
> (b) by a process in which the contents of a document
> (i) recorded by photographic, electronic or other means; or
> (ii) stored on a data storage device, are reproduced, whether in the same form or in some other form; or
> (b) in any other way.

Section 57 (3) of the South Australia Act states that If a court admits or refuses to admit a document under this section, the court must if so requested by a party to the proceedings, state the reason for its decision. Section 57 (4) of the South Australia Act

further adds that in determining whether a particular document accurately reproduces the contents of another, a court is not bound by the rules of evidence and, in particular, the court may rely on its knowledge of the nature and reliability of the processes by which the reproduction was made (South Australia Act, 1929).

5.4.5 South Africa Legal response to Admissibility of Digital Evidence

The South Africa digital evidence admissibility is found in Computer Evidence Act 57 of 1983. The Computer Evidence Act 57 of 1983 was enacted to address the criteria for admissibility of digital or electronic evidence in legal cases since there were no provisions for admissibility issues relating to computer printouts in the Civil Proceedings Evidence Act 25 of 1965. The Act requires investigators to tender in computer printouts in legal court with an affidavit and the purpose is for the judge or the court to verify the identification of a printout, sources of the evidence, and certification that the computer from which the printout was made was in good working order. In addition to this, the Electronic Communication and Transactions Act 25 of 2002 have since been passed and this Act regulates matters regarding the use of electronic evidence in both criminal and civil proceedings. The Electronic Communication and Transactions Act 25 of 2002 applies to transactions conducted over the internet or electronic communications means. This law addressed categories of electronic evidence that courts may determine to admit in the courtroom. The Electronic Communication and Transactions Act 25 of 2002 is the most important legislation dealing with electronic evidence, this view is confirmed by Van der Merwe *et al*. (2008:75), who mentions that the criminal provisions in the Electronic Communication and Transactions Act 25 of 2002 "so far, are the mainly significant legislative countermeasures against computer crimes in South Africa" The Act deals with the presentation of electronic information and can be used in conjunction with the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002, which deals with the collection, preservation and reporting of electronic information. The Electronic Communication and Transactions Act 25 of 2002 specify or set out data messages and signature shall be deemed to produce the same legal effect as written documents. Section 15 (1) of the Act highlights the specific rules of admissibility and evidential weight of data messages and it states that: (1) In any legal

proceedings. The rules of evidence must not be applied to deny the admissibility of a data message. In evidence-

(a) on the mere grounds that it is constituted by a data message; or
(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain because it is not in its original form.

Section 15 (2) of the Act also highlights that information in the form of a data message must be given due to evidential weight. Section 15 (3) of the Act further states that: in assessing the evidential weight of a data message, regard must be had to-

(a) the information contained in the data message is accessible so as to be usable for subsequent reference:
(b) the data message is in the format in which it was generated. sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
(c) the origin and destination of that data message and the date and time it was 15 sent or received can be determined.

However, in assessing the originality of data messages by judges in the South African courtroom, Section 14 of the Act stipulates that:

(1) Where a law requires information to be presented or retained in its original 25 forms, that - requirement is met by a data message if:

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed the assessment in terms of subsection (2); and
(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1(a), the integrity must be assessed-

(a) by considering whether the information has remained complete and unaltered. Except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display:
(c) in the light of the purpose for which the information was generated; and
(d) having regard to all other relevant circumstances.

Section 15(4) provides an exception to the manner of proof and evidential weight ordinarily to be accorded to a data message. In *Ndlovu's* case, the court held that s 15(4) does not require a qualitative inquiry to be made in terms of s 15(2) or (3) in regard to the

weight to be attached thereto (173). It provides for its weight, namely that the facts contained therein will be rebuttable proof – namely if not rebutted, then they will stand as evidence. In *Trend Finance (Pty) Ltd and Another v Commissioner of SARS and Another* [2005] 4 All SA 657 (C) the electronic evidence adduced was rejected because it did not satisfy the definitional requirements of a 'printout' in terms of s 15(4). The Electronic Communication and Transaction Act 25 of 2002 as asserted by Hofman (2006:3), is based on the model law and as such conforms with international law and standards. Thornton, Carrim, Mtshaulana and Reburn (2006:264) posit that the ECT Act was enacted to provide national legislatures with a guide of an internationally acceptable set of laws to create a more secure legal environment for electronic commerce.

5.5 COMPARATIVE AND LEGAL ANALYSIS

Although Ghana does not have a law promulgated for Computer Evidence, the other laws that judges and prosecutors are using for the prosecution of cases involving digital evidence lack comprehensiveness and breadth of scope. The Electronic Transaction Act 772 of 2008 and Evidence Act 1975 are deficient and exhibit an incomplete understanding of digital evidence for the reason that the Electronic Transaction ACT 772 of 2008 only states admittance of electronic contracts and messages that are sent, receive, stored, and generated electronically. The Evidence Act 1975 (N.R.C.D 323) on the other hand did not specifically state the admittance of e-mail and computer-stored evidence. Meanwhile, many types of computer-generated evidence which comprise log files, metadata, deleted files or data, computer time artefacts, and hash values are far off the scope of the Electronic Transaction ACT 772 of 2008 and Evidence Act 323 of 1975 and these makes them pertinent to a limited or few range of cases. Furthermore, the Ghanaian Cybersecurity Act 1038 of 2020 and Criminal Procedure Act 30 of 1960 do not give a clear and detailed to address certain forms of digital evidence even though it permit judges to exercise broad discretion and admit evidence at trial and the actual implementation to practice are affected by the fact that many judges and prosecutors at the courts lack the skills, training and knowledge in the information and Communication technology law field and as a result judges will be slow and uncertain in their acceptance

of digital evidence. However, the lack of computers and Information Technology infrastructure knowledge among judges, lawyers, and prosecutors in Ghana are a major concern in this field. There is no common set of rules and guidelines for the presentation of digital evidence in Ghana compared to other countries like the United States, United Kingdom, Australia and South Africa." In addition, the legal systems and courts in Ghana are still ill-equipped to deal with digital evidence in its legal court and the entire Act stated there was no level of standardization for digital evidence.

By contrast, United States, United Kingdom, and Australian laws plentifully provide the foundation and basis for digital evidence acceptance on an exact copy by encompassing what constitutes a digital document and providing judges with guidelines for digital evidence validation. The United States Federal rules of evidence (FRE) lays down rules regarding evidence admissibility. The United Kingdom Civil Evidence Act 1995 was enacted to allow a judge to admit electronic evidence admissibility at a court of law. The South Africa Computer Evidence Act 57 of 1983 was enacted to address the criteria for admissibility of digital or electronic evidence in legal cases.

The analysis and review of Ghanaian laws lack the quality required to deal with digital evidence admissibility and it needs to be addressed if legislation is to achieve its objective of admitting evidence. The inadequacies are both juridical and non-juridical which fall in technology, litigation support, education and training. From a juridical point of view admissibility of digital evidence or electronic evidence is scattered over a wide range of written laws or statutes which lack all elements of digital evidence admissibility and uniformity. As a result, the Evidence Act 1975 (N.R.C.D 323) must be revised or amended to correctly contain all the digital evidence admissibility structure and recognise computer-generated evidence and admittance of the exact copy into evidence in lieu of original copy. From non-juridical point of view, courtroom must be furnished and equipped with high-tech infrastructural facilities because they are necessary for presentation and evidence recognition. Training and education are also need to enhance and broaden the knowledge of lawmakers, prosecutors, and judges so they can fully understand digital evidence. In Ghana, the court systems and the judge's knowledge of technological infrastructure including digital evidence features are unripe and are far from meeting the

United States, United Kingdom or Australian Level and this is because of the rarity of studies addressing cybercrime issues and insufficiency of opportunities to adjudicate cases involving digital evidence.

5.6 CHAPTER SUMMARY

In less than two decades, society has adopted information and communication technology and personal computers have not only been a part of the conduct of criminal activities but also part of the evidence in their criminal prosecution. The distinctive features of electronic infrastructure or information and communication technology systems make the classical laws on digital evidence inappropriate to some degree when day-in and day-out investigators, lawyers, prosecutors and judges are being confronted with criminal issues involving digital crime. Digital evidence is volatile and can be defiled or tainted during collection processing, handling and preservation thereby decreasing its admittance in legal court during the litigation process. There have been several battles and complex scenarios on digital evidence admissibility by prosecutors and defendants. However, metadata and hash values will remain and continue to be the most important factors to enable digital forensic investigators and prosecutors in defending and proving digital evidence integrity in the courtroom. Given this, reliable information such as training and education should be given to judges and prosecutors to enhance their knowledge of digital evidence integrity techniques. The development of digital crime evidence lab by law enforcement has been slow and lack national and regional planning and coordination. These make it difficult for law enforcement to do the extraction of digital evidence during the prosecution process in other part of the country. Because the Ghanaian digital evidence admissibility legislation is scattered all over a wide range of statutes make its lack of comprehensiveness is evident thereby restricting judges to accept digital evidence in a particular type of dispute or ligation. Although the Evidence Act 1975 (N.R.C.D 323) grants the judge to accept and evaluate digital evidence there are no precise or uniform provisions and guidelines for all judges to follow in their acceptance and evaluation of digital evidence. Therefore, judges should be provided uniform guidelines, appropriate

training, guidance and comprehensive laws on how to deal with digital evidence acceptance, evaluation and authentication in the courtroom.

CHAPTER SIX

RESEARCH FINDINGS, CONCLUSIONS AND RECOMMENDATION

6.1 INTRODUCTION

The aim of this study is to examine and identify legal issues and challenges relating to virtual criminal investigations and to do a comparative legal study of other jurisdictions. This research came about as a result of virtual crimes, internet vulnerabilities and criminal activity in Ghana and the necessity to enhance investigation skills by law enforcement and investigators and to improve insufficient laws to prosecute cybercriminals. The study focused on Legal issues and investigative procedures, approaches and challenges that are being faced by law enforcement and investigators in Ghana. The study also focused on searching and seizing virtual or digital evidence without tempering or compromising its integrity or credibility. The focus was also on the standard or requirements for admitting electronic evidence at trial. The digital or virtual criminal investigations process require investigators or law enforcement to identify, collect, handling and preserve virtual evidence in manner that is able to withstand any legal scrutiny at trial. Law enforcement and Investigators need to be properly trained and skilled in using the required toolkit, have in-depth knowledge in legal procedures on searching and seizing virtual or digital evidence and the legal requirements in handling and authenticating the digital or virtual evidence. Understanding the laws and regulations governing electronic communications,

virtual crime, and data retention require the continuous acquisition of new knowledge, methods, and tools for virtual criminal investigations. One of the important roles in any virtual criminal investigation in this century is digital evidence. Unfortunately for the investigator, the information super highway or the World Wide Web was designed with much focus on robustness rather than security and traceability. This increases the complexity and uncertainty of digital forensic investigation and represents a formidable challenge for digital criminal investigators. From the study, the researcher has observed that law enforcement and investigator tend to focus on traditional or document-based evidence because their knowledge in dealing with electronic evidence is limited. To address the aim and seek for answers, the researcher formulated five (5) research questions based on the specific objectives detailed in 1.5 above:

6.2 RESEARCH FINDINGS

The findings below are all based on the research method explained on 1.9.1 above which is legal research methodology, criminal justice and investigation research methods approach that it is very appropriate to elicit the relevant information for the research question and objective. Information obtained during the gathering of data were through legal and court cases on cybercrime investigations, government policy documents on cybercrime, digital forensic evidence policy documents, legal framework documents, cybercrime journals and other literature study on the topic. These findings are aimed at improving the procedures that are followed with regard to virtual criminal investigation and gathering of electronic evidence for prosecution. the researcher made use of research questions to spell out exactly what is to be investigated and this assisted the researcher to address the problems that were identified with regard to legal issues and challenges on virtual criminal investigation in Ghana. The following are the findings of the research:

6.2.1 RESEARCH QUESTION ONE (1)

- **What are the legal issues and challenge of virtual criminal investigation in the current laws governing cybercrime?**

6.2.1.1 VIRTUAL CRIMINAL INVESTIGATIONS CHALLENGES

The research established that virtual crime is any violation of criminal law that involve knowledge of computer technology for their perpetration, investigations, or prosecution. Pardis, Manap, and Taji (2013:207) opine that the rapid growth of technology is beneficial to humanity, and it has also given rise to cybercrime. This study proves that virtual attacks have become a pressing issue due to the deficiency of a consistent international treaty and the lack of international resolve. The research shown that virtual crime investigation brings unique challenges which are not encountered in most traditional crime investigations. It was evident that the technical nature of virtual criminal investigation makes this approach nearly impossible. Due to the technical nature of virtual crime or cybercrime, only the prosecutors who can handle virtual crime are involved. Moreover, virtual crime can be automated in a way that a traditional crime cannot. As a result, law enforcement agencies are forced to prioritize and investigate the most serious crimes. It was emerged that due to the nature of flash memory, and lack of sufficient protocols in place to outline effective data retrieval technique for solid state discs, and universal serial bus flash drives, virtual or digital forensic examiners face many challenges that sometimes impede their ability to operate successfully. Karyda and Mitrou (2017) reveal that procedural problems arise from the lack of standardization, as well as the lack of theoretical framework for the field of digital forensics. Using ad-hoc methods and tools for the elicitation of digital evidence can limit the reliability and credibility of the evidence, especially in a crime prosecution process where both the evidence and the processes used for collecting it can be disputed (Karyda & Mitrou 2017).

Additionally, Alison et al (2018) further adds that, to the countless technical issues that virtual crime investigators face, there are also numerous legal matters to consider. The low-level skillset of computers among law enforcement employees and prosecutors is one of the technology challenges law enforcement agents face in the investigation and prosecution of cybercriminals (Institute of ICT Professional Ghana, 2018). While traditional crime investigation does not require prior investments of time, yet can lead to the arrest of the criminal, cybercrime investigations require an investment of time, but may result in no arrests. The estimated time for atypical cybercrime is several months

and years depending on the nature of the crime committed (Institute of ICT Professional Ghana, 2018). The increasing incidents of cyber-attacks against sovereign states and their critical information infrastructures necessitate a global response. Regional and bilateral agreements and local legislation are not sufficient to deter cyber-related attacks (Pardis *et al* 2013:207). Therefore, international law is a necessary tool to enable the global community to deter cyber threats in its various jurisdictions. Bantekas (2010:265) posits that nations must come up with self–regulatory legal mechanisms to combat the misuse of new technologies, such mechanisms need to be supported by international agreements and appropriate national legislation.

The nature of the internet gives the ability to the user to disguise their identity, leading to inherent difficulties in determining the states that fail to prevent an attack from being originated within their borders (Pardis *et al* 2013:207). Therefore states must cooperate with each other to share information in order to attribute attackers (Grosswald, 2011: 1151). Terrorist groups have turned from conventional attacks to cyber-attacks since they can now launch their attack from far distances and disregard entire borders and physical barriers. Cyberspace has become a fertile ground because of its lack of boundaries. Universal jurisdiction may be created by treaty regimes, or are binding on the states that are parties to them (Nadya, 2001:242).

6.2.1.2 LEGAL ISSUES IN VIRTUAL CRIMINAL INVESTIGATIONS

It has emerged from this research that there are legal issues that are particularly acute in the context of the internet privacy, since it provides a new source of data collection agencies. It was established in this research that the Internet is notorious for giving its users a feeling of anonymity when in reality they are highly visible and open to violations of their privacy. From the court cases that the researcher analysed and are found in this research, it became evident that privacy issues have always been a major concern in digital or computer forensic investigation and in other cases that are not pertaining to computers. It emerged that digital forensic investigators have faced challenges in finding the balance between retrieving key evidences and infringing user privacy. For example, the research found that the United States (US) Fourth Amendment creates a right to be

free from unreasonable searches and seizures and serve as the deciding factor in all governmental investigations. Any evidence obtained in violation of the United States (US) Fourth Amendment is inadmissible in a court law. Virtual crime investigation constitutes an intrusion on an individual's reasonable expectation of privacy. Constitutionally, the concept of reasonable expectation of privacy, which was derived from the US Constitution Fourth Amendment primarily, serves as a defensive instrument against warrantless search and seizure of private property and also against illegal internet surveillance. The research established that the Fourth Amendment protection for physical objects was extended to include intangible assets, such as conversation and Internet activities, by the United State Supreme Court's prominent decision in *Katz v. United States (1967).* Katz 'was convicted of transmitting wagering information by telephone in violation of federal statute. In the Katz Case, the information was overheard by an FBI agent who had attached an electronic listening and recording device to the outside of the public telephone booth where Katz had made his call. The Court found by seven votes to two that "the Fourth Amendment protects people, not places. Nevertheless, the concept of a reasonable expectation of privacy, which was first formulated by Justice Harlan who deliberated in the case, has become a test of privacy. This test requires an actual subjective expectation of privacy that society is willing to recognise as acceptable as well as a balance between the people's right to privacy and the government's interest in crime prevention (Doug *et al* 2011). In *Katz v. United States, 1967*, the United States Supreme Court ruled that intrusion through technology counted as search and extended Fourth Amendment protection to any area that an individual has a reasonable expectation of privacy. Also in a matter of *United States v. Kim 2015,* the laptop of owned by Kim was seized by the government as he was leaving on an international flight in 2012. There was a copied and searched on the laptop drive which revealed evidence of arms dealing. The evidence was inadmissible by the judge and dropped the case at the federal court by saying that the investigator lacked authority to conduct a warrantless search, and had violated Kim's right to privacy. The court cited the Supreme Court's observation in *Riley v. California,* 573 U.S. 373 (*2014)* stating that Riley, made it clear that the breadth and volume of data stored on computers and other smart devices make today's technology

different in ways that have serious implications for United States (US) Fourth Amendment analysis.

In matter of *United States v. Ganias* 12-240 (2d Cir. 2016) the Second Circuit of Appeals detailed the complexity of search and seizure of digital evidence. In earlier proceeding the court agreed that the government had violated Ganias" Fourth Amedment rights by holding evidence that was unrelated to the scope of the original warrant and overturned the conviction. Additionally they ruled that the government cannot indefinitely retain every file on a computer for future use. During an embank session, the court declined to rule on the matter of the Fourth Amendment violation stemming from the retention of the mirror image, refused to suppress the evidence, and reversed the earlier decision. However, two critical observations were mentioned by the judges: One, electronically stored data is not always in one location but “fragmented” on a storage device, potentially across physical locations, and two, metadata can be stored in various location across a system, supporting the imaging of an entire drive. Also, in the case of *United States v. Simnons, 206 F.3d 392 (2000)* a government employee working for the Central Intelligence Agency was suspected of using his office computer to download pornography. The CIA, acting without a warrant, remotely accessed the computer, and discovered photos of child pornography. In the criminal case that resulted, Simmons tried to suppress those photos, claiming a violation of the Fourth Amendment. However, the CIA had an Internet use policy that allowed it to “periodically audit, inspect, and/or monitor … users" Internet access”. The Court determined that in light of this formal policy, the employee had no reasonable expectation of privacy hence no warrant was required for the government search. No warrant is needed when the target consents to a search of his/her computer. No warrant is needed where a third party, such as a spouse, parent, employer or co-worker consents to the search, so long as the third party has equal control over the computer. No warrant is required when probable cause exists but there is an “emergency”, leaving no time or opportunity to obtain a warrant. An example is *(United States v. David, 756 F. Supp. 1385 (1991*), where agents observing the target deleting files immediately seized the computer. In considering the application of criminal law to instances of computer-related crime investigations in the United Kingdom, a variety of issues arise (Lloyd 2017). In the early days of computer-related conduct, any criminal

charge in the United Kingdom was required to be brought under the traditional legal headings. Lloyd (2017:211) asserts that incidents where damage was caused to the contents of a computer, either directly or by causing it to be infected by a computer virus were successfully prosecuted as a species of criminal damage under the criminal damage Act 1971. Starting in the 1980s, a trend began in the United Kingdom for the adoption of computer-specific status to combat cybercrime. The law commission in the United Kingdom recommendations for reform of this area had resulted in the passing of the Computer Misuse Act 1990, which due to the criticisms of the reasoning in *Cox v Riley,* had effectively removed such cases from the ambit of the Criminal Damage Act 1971. In the United Kingdom, there has been debate about the extent to which existing laws were adequate to deal with the distribution of pornography on the Internet. This included the extent to which they were capable of dealing with instances in which children are exposed to material intended only for an adult audience, as well as instances in which the internet was used to propagate child pornography.

Although Ghana does not have a Bill of rights, various aspects of privacy in Ghana, and up till now are enshrined in the 1992 Constitution. Article 18(2) provides citizens with a fundamental right to privacy. The Article provides that "no person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or the protection of the rights or freedoms of others." Communication privacy in Ghana is established and maintained by the Electronic Communications Act 775 of (2008) which also, highlights the declaration of personal information and states that a network operator or a service provider who is a holder of a "Class Licence" shall not use or permit another person to use or disclose confidential, personal or proprietary information of a user, another network operator or service provider without lawful authority unless the use or disclosure is necessary for the operation of the network or service, the billing and collection of charges, the protection of the rights or property of the operator or provider, or the protection of the users or other network operators or service providers from the fraudulent use of the network or service. A person who intentionally uses or discloses personal information in contravention of the

Act commits an offence and is liable on summary conviction to a fine of not more than one thousand five hundred penalty units or a term of imprisonment of not more than four years or both.

There is no section in Act 775 that specifically addresses the rules of cyberspace, surveillance, searches and seizures. The Ghanaian Electronic Communications Regulations (2011) specifies that the principle of privacy and secrecy in electronic communications applies to the National Communications Authority, operators of electronic communications networks and providers of electronic communications services. The Electronic Communications Act 775 of (2008) and Electronic Transactions Act 772 of (2008) include no provision or mechanism to guide law enforcement officers or investigators on when there may install and run surveillance systems or tracking devices for investigation purposes.

Lack of trust, coupled with ineffective anti-terrorism strategies and flaws embodied in Carniovere, forced privacy groups to challenge law enforcement efforts on fighting cybercrime (Goffrey 2002:155). For example, the FBI launch an initiative called the Federal Intrusion Detection Network (FIDNET), designed to fight cybercrime by monitoring government computers for security breaches and the controversial Carnivore Internet surveillance system collided with the principles of privacy advocate group, the latter argued that such initiatives, which aim to curb illegal activities on cyberspace, would weaken privacy and had amorphous limits, despite the legitimate need to tap and monitor Internet traffic. The Australian Law Reform Commission (2014) posits that the Australian Constitution establishes a federal system of government in which powers are distributed between the Commonwealth and the six states. It includes a list of subjects about which the Australian Parliament may make laws. That list does not include privacy expressly but this does not mean that the Australian Parliament has no power in relation to privacy. The principal piece of federal legislation regulating privacy in Australia is the *Privacy Act*. The *Privacy Act* was passed partially in reliance on the basis of the Australian Parliament's express power to make laws with respect to 'external affairs (Australian Privacy Act 1988). The Australian privacy rights are contained in a variety of Federal and

State legislative provisions. Although, Australia does have a bill of right, various aspect of privacy legislation has witnessed major modifications. In the Federal sphere, the law is codified by *Criminal Code Act 1995* (Cth) which was amended in 2001 by the *Cybercrime Act 2001(Cth)*.

A common law tort for invasion of privacy has not yet developed in Australia, despite the High Court leaving open the possibility of such a development in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd in 2001.* A tort of invasion of privacy has been recognized by two lower court decisions: *Grosse v Purvis* in the District Court of Queensland and *Doe v Australian Broadcasting Corporation* in the County Court of Victoria. However, both cases were settled before appeals by the respective defendants were heard. No Australian appellate court has confirmed the existence of this tort, and the judgments of several courts suggest that the common law is unlikely to recognize the tort in the foreseeable future: commenting on *Grosse v Purvis, Heerey J* and *in Kalaba v Commonwealth of Australia* held that the weight of authority was against the proposition that the tort is recognized at common law; in *Chan v Sellwood; Chan v Calvert,* Davies J described the position on the existence of the tort at common law as 'a little unclear. The telecommunications (Interceptions) Act 1979 and Act 1988, until recently, protected individual privacy against illegal communication interception, alteration, and disclosure of personal information.

In South Africa, Section 14 is the privacy clause in the Constitution and it reads as follows: Everyone has the right to privacy, which includes the right not to have- (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed. This section provides for a general right to privacy, together with a direct guarantee of a right to privacy with regard to home life, private communications and the prohibition of unlawful entry and search. The advancement of South Africa through technology and innovation has seen the government of South Africa passed the Electronic Communication and Transactions Act 25 (ECTA 2002) to deal with the fast increase in cybercrime. The spirit of Act 25 (2002) is captured in the preamble which states as its objective "provide for the facilitation and regulation of electronic communications and transactions; for the development of a

national e-strategy for the Republic; to promote universal access to communication and transactions and the use of electronic transactions; to provide for human resource development; to prevent abuse of information system; to encourage the use of e-government service, and to provide for matters connected therewith" (ECTA 2002, Act 25, Preamble). Section 86 respectively of the Electronic Communication and Transactions Act 25 (ECT) seeks to criminalize illegal access and unauthorized modification of information as well as the possession and distribution of hardware devices and software programs that facilitate an offender's action of cybercrime. ECTA sufficiently deal with jurisdiction, the acceptability of data messages, the admissibility of electronic signature, as well as the regulation of cryptography (ECT, part 1, and 2 of the Act respectively). ECTA has some specific provisions that specifically speak to the issues of cyber activities prevalent in the world today. Section 86(part 1) of the Act criminalizes all forms of hacking, while Section 88(part 1) of the Act also criminalizes any attempt by criminals to gain unauthorized access. The country in its attempt to fight cybercrime on a global scale has formed an alliance with the European Cybercrime Treaty which encourages member states to make laws to fight the menace. Other laws such as the Electronic Communications Act 9, (Act 36 of 2005) and the State Information Technology Agency Act10 (Act 88 of 1998) are used in South Africa to curb the cyber menace.

6.2.1.3 JURISDICTIONAL ISSUES AND CHALLENGES IN VIRTUAL CRIMINAL

It is obvious from the research that portability and connectivity of computer systems lead to questions about jurisdiction. The research has illustrated that the legal power of law enforcement agencies to investigate and prosecute crime is limited to the territory of the nation or state. This rule follows the principle of sovereignty in international law. It became evident that, the official authorities of the state or country in which the digital evidence is located have exclusive powers to access and secure the evidence. It was established that when a law enforcement agency accesses and secures evidence located within the territory of another state, it exceeds its powers and violates the sovereignty of the other state. It was revealed that virtual crime investigation for electronic evidence must meet the formal evidentiary requirements of the courts if it is admissible in a court of law in a particular jurisdiction. The research found that jurisdiction in virtual crime investigation or

digital crime investigation is tricky as the legal system in one jurisdiction differs from another in the location of data and information. Brenner, Koops, and Bert-Jaap (2004).reveal that the cybercrime statutes that have been enacted over the past decades in numerous countries show varying and diverging jurisdiction clauses. Brenner *et al* (2004) contend that Jurisdiction conflicts abound, both negative (no state claims jurisdiction) and positive (several states claim jurisdiction at the same time). Above all, it is unclear just what constitutes jurisdiction: is it the place of the act, the country of residence of the perpetrator, the location of the effect, or the nationality of the owner of the computer that is under attack. André (2018:114) state that the enforceability of jurisdiction clauses and, more generally, the issue of which court should settle the dispute are significant both in practical and substantive terms. There are formal procedures for international cooperation against crime, covering different aspects of investigation and prosecution, such as assistance to seek, arrest, and extradite a suspect, and obtain witness or expert testimony and other forms of evidence for the benefit of a criminal investigation in another state. International cooperation must proceed along procedures for mutual legal assistance and or procedures for international police cooperation. As a main rule, the procedure for mutual legal assistance must be applied when evidence is sought to be obtained by coercive measures. The Council of Europe Cybercrime Convention seeks countries to build on the principle of comity and require the parties to cooperate and assist each other when a cybercrime investigation is urgently needed or to be conducted. Article 25(1) specifies with respect to the collection of evidence in digital form of criminal offences the (Council of Europe cybercrime convention). André., *et al* (2018:213) point out that close international cooperation is needed in order to counteract trans-border digital crime and, generally, collect digital evidence which is relevant in most criminal investigations and also harmonisation of national substantive and procedural criminal law is a precondition for effective international cooperation, along with recognition of the fundamental human rights and the rule of law.

6.3 RESEARCH QUESTION TWO (2)

- **What are the cybercrime legislation principles, and their application towards digital forensic investigation and admissibility of virtual evidence for prosecution?**

6.3.1 ADMISSIBILITY OF DIGITAL EVIDENCE IN THE COURTROOM

The research has shown that it is officially compulsory for all law enforcement or virtual criminal investigators to have a sound knowledge of all the legal requirements and principles applicable towards virtual or digital forensic investigation and gathering of electronic evidence. It has emerged from this research that there are established virtual crime or cybercrime legislation principles and internationally recognised general standards and best practice procedures for collection of electronic evidence and admissibility of virtual evidence or digital evidence in the courtroom It was established from the research that the Electronic Transactions Act 772 of 2008 does not provide guidelines for the collection of electronic evidence and in Ghana there are no procedures that have been tested by courts on the collection, preservation and analysis of electronic evidence. It was established in this study that the purpose of a courtroom is to administer justice, and the role of digital investigators in this context is to present supporting facts and probabilities. The research emerged that court depends on the trustworthiness of digital investigators and their ability to present technical evidence accurately, it is their duty to present findings in a clear, factual, and objective manner. Also, the it proven that courts are concerned with the authenticity of the digital evidence they receive which requires digital investigators to be honest and forthright

As indicated by Swanson et al (2019:682) admissibility is the essence of the rules of evidence. The rules of admissibility protect the trier of fact, generally a jury, from hearing improper evidence that may be unreliable or untrustworthy and that may prejudice the case unjustifiably against the defendant (Swanson *et al* 2019:682). The majority of the rules of evidence deal with what is admissible. Questions of admissibility are decided by

the judge, and these decisions are made outside of the hearing of the jury. In the case of *R. v Fowden and White (1982)*, the Court of Appeal held that a video film showing activities that were consistent with the acts of theft had been improperly admitted. The prejudicial value outweighed its probative effect because the witnesses that identified the accused knew them from a similar case of theft that occurred a week after the events recorded in the video film, and the defence was therefore not able to test the accuracy of the identification without causing prejudice and embarrassment. Investigators processing evidence must realize that, in addition to being pertinent, the evidence must meet certain standards to be admitted. It is easy enough to claim that a fingerprint was found in a suspect's computer, but it is another matter to prove it. When guilt or innocence hangs in the balance, the proof that evidence is authentic and has not been tampered with becomes essential. Digital evidence is admitted in most jurisdictions, subject to country-specific legal rules of evidence (Roffeh 2014:24). Antwi (2018:51) posits that the global acceptance of digital evidence as a form of evidence marks a significant milestone for the development of digital forensics but specific challenges remain and face some hurdles when presented in court. With regard to the above challenges, cautions must be taken when presenting electronic evidence in court. This is because electronic evidence can easily be manipulated and distorted and therefore can always be put through to serious legal perusal.

6.3.1.1 Rules of Admissibility for Evidence in Courtroom

It is established in this research that the principles for the admissibility of evidence are based on rules. In a court proceeding, the jurors or judges adhere to high standards of proof when presenting evidence. Therefore, the legality and reliability of evidence are some of the essential requirements that will be considered by the judiciary when deciding on the admissibility of evidence. Swason *et al* (2019:682) recommend the following rules governing evidence admissibility in court.

6.3.1.2 Relevance

Swason *et al* (2019:682) posit that the rules governing the admissibility of evidence require that the evidence must be relevant, that is the evidence must have a bearing on the issue in the case being tried. The relevance of a particular piece of evidence can easily be determined by the answer to this question: “Does this piece of evidence have productive value?” alternatively stated, “Will it aid in proving or disproving a particular point that the jury should consider in determining the guilt or innocence of the defendant and if it cannot throw some light on the case, it is irrelevant?”

6.3.1.3 Test of Materiality

Test of materiality is another important factor or key that governs the admissibility of evidence. Assuming that a particular piece of evidence is relevant if it is such an insignificant and unimportant point that its admissibility will not affect the outcome of the case, it may be inadmissible. Thus, materiality deals with the importance of the item of evidence in question. A fact is material if it will affect the result of a trial. For example, a defendant is charged with a crime committed in a hotel and was captured by Closed Circuit Television (CCTV) at ten o'clock (10:00PM) at night. State witnesses testifying that they saw the defendant at that time are relevant and material. Defence witnesses testifying that the defendant was at another place miles away are also relevant and material to the fact in issue.

6.3.1.4 Competence of evidence

Swanson et al (2019:683) state that the test of competence of evidence relates to the evidence's legal significance to the case, because of certain statutory requirements or other rules of evidence, a particular item of evidence may not be admissible. For example, there is a rule of evidence to the effect that the defendant’s character cannot be attacked by the prosecution unless and until the defendant tries to show that he or she is of good character. Hence, unless the defendant did proceed in this direction, any attempt by the

prosecution to introduce evidence of the defendant's character would be inadmissible on the grounds of incompetence.

The competence of digital evidence must be established as a condition of admissibility. This is done through a process known as laying a foundation. For instance, the admissibility of an electronically recorded conversation would have to be prefaced by testimony about the date, time, place, and circumstances under which the recording was made, the satisfaction of legal requirements in the making of the recording, proper identification of the voices on the tape, assertions about the functioning of the recorder and tape at the time of the recording and assurance about the absence of editing or modification of the tape.

6.3.1.5 Competence of Witnesses

With the advent of the rules of evidence, procedures had to be established for requiring the presence of people who possessed knowledge of the facts of the case. The success or failure of a criminal investigation is often ultimately measured in terms of the quality and effectiveness of an officer's, witnesses or expert witness presentation to the court or jury. Digital evidence expert witnesses have come to play an extremely important role in terms of courtroom testimony owing to the many advances in information and communication technology systems and related devices. Digital evidence expert witnesses have conducted evidence collection investigations on computers, mobile devices, and other media, with the results of these investigations subsequently being presented as crucial evidence in the courtroom. The expert witness on digital evidence is responsible for the collection, documentation, preservation, interpretation, and analysis of the evidence contained in the suspect's computer and related electronic devices. Accordingly, this person or individual is often subpoenaed to testify about the evidence, including how it was discovered, created, obtained, and if there are modifications, that may have occurred either intentionally or accidentally to the evidence during the recovery process. In United *States v. Kassimu,* (2006 WL 1880335 5th Cir.) district court correctly found that computer records were authenticated based on the Postal Inspector's description of the procedure employed to generate the records.

Moreover, Rule 705 of the Federal Rules of Evidence in the United States that the expert may testify in terms of opinion or inference and give reasons therefore without first testifying to the underlying fact or data unless the court requires otherwise. The expert may in any event be required to disclose the underlying facts or data on cross-examination. As such, unlike technical or scientific witnesses, expert witnesses are allowed to provide testimony that includes their opinion of any observations made during the investigations. A party is required to disclose to the other parties the identity of any witness it may use at trial to present evidence under Federal Rules of Evidence 702, 703, or 705. According to Federal Rules of Civil Procedure Rule 26a (2B), the disclosure must be accompanied by a witness report that is prepared and signed by the potential technical or expert witnesses, which contains the following information:

(a) All the opinions to be expressed that are relevant to the case, the basis for these opinions, and any exhibits that may be used to summarize or support these opinions.
(b) The individual's qualifications, including any publications made that are relevant to the issue the individual is providing an opinion on
(c) The cases in which the individual served as an expert witness during pretrial and or court proceedings.

Swason *et al* (2019: 694) contend that regardless of their knowledge of the facts of a case, certain individuals are not permitted by law to testify for or against a defendant in a criminal case. To establish the competency of a technical or expert witness to participate in a trial, a thorough examination of that person's background and credentials is required (Marras, 2015:362). This occurs through a process known as *voir dire*. Marras (2015:362) state that the phrase *voir dire* comes from medieval French and roughly means “to speak the truth,” and describes the preliminary examination used to determine whether a witness or juror is competent or qualified. During this process, the opposing party’s attorney will attack the credibility of the individual providing the testimony. Primarily, the attorney will attack the credentials, methods, used, and any oral or written statements made by the witness. Often, the opposing party’s attorney may attack the qualifications of the expert, as opposed to his or her methods or interpretation of the result.

During the voir dire process, the following details about the witness must be verified (Marras, 2015:362):

(a) Name
(b) Title
(c) Employment history (Position held, length of position, and duties in each position
(d) Current occupation including the position held, length of time in the current position
(e) Any specialization in the current field of employment (e.g in the field of security, an individual may specialize in protective services operations, whereas in the field of computer forensics, an individual may specialize in network forensics)
(f) Employment address
(g) Education, including any degrees, held, in which subject(s), from which college or university
(h) Licenses and membership of profession (from which association, recognise the body, and in which field)
(i) Specialized training and board certification as a specialist in the field.
(j) Any teaching or lecturers given, including the date and place of where teaching or lectures took place
(k) Publication in the individual's field of specialization
(l) Cases where the individual served as a technical or expert witness in pretrial or court proceedings.
(m) Honour, award or any other special achievements in the individual's field
(n) Consulting the individual may have provided to private and or public agencies.

During the *voir dire* process, it would be unwise to rely on the resume or curriculum vitae (CV) provided by the potential expert witness for all this information because individuals

frequently embellish the information provided in these documents. Instead, witnesses should be subjected to a thorough background investigation. One can begin this process by conducting research on the potential witness and there are several resources available to help attorneys find the right expert, evaluate their credibility, and assess the admissibility of their testimony (Marras, 2015:362. One such resource is the Technical Advisory Service for Attorneys (TASA) in the United States which serves legal professionals by providing them with experts to assist them in various areas of litigation, including case evaluation and testimony. Public records searches can also provide information about the individual's aliases, maiden name, relatives, criminal records, property, military service, address history, phone numbers, and email addresses. All licenses, professional certifications and training listed for the witness should be checked as well by contacting institutions, agencies or organisations that provided them. Professional license information may also be found on websites called Black Book Online for free or with a fee.

Moreover, the publication reported by the witness should be verified. If the individual has published an article, to search for this publication, the investigator can go directly to the publisher’s website and browse for the article in question. Insight into the personal and professional lives of witnesses is also sought. Some information on these individuals may be found on social and business networking sites such as Twitter, Facebook, LinkedIn. Prior cases in which expert witnesses participated should also be checked, for example, to reveal any existing biases or challenges to the testimony they had provided, their methods, or their qualifications as experts. The prior testimonies of a potential witness should be reviewed to reveal that an individual's strengths and weaknesses are inadequate tools for witness due diligence. The interrogation and background check to which the potential expert witness is subjected and quite intense because acceptance of an unqualified expert is considered grounds for overturning the verdict in a higher court (Girard, 2012:52). A prime example of what happens when the qualifications of an expert are not checked can be found in the case of Fred Zain (West Virginia State Police crime laboratory) 1977). Zain was employed as a forensic expert by the West Virginia State Police department in their crime laboratory and testified in hundreds of criminal cases. Zain, however, was never qualified to perform forensic work. His educational transcripts

revealed that he was a mediocre student and had failed chemistry. Despite his poor academic background, he was employed as a chemist at the Department of Natural Resources after completing his education. His employment background as a chemist was one of the main reasons his lab chief at the time, Ray Barber, claimed that he felt that he did not need to check Zain's background before hiring him. After reviewing 189 cases in which Zain provided a report and or testimony, a court warned that any testimony or documentary evidence offered by Zain at any time should be deemed invalid, unreliable and inadmissible.

Another expert witness who lied about her credentials was Carolyn Ridling. In 2008, Ridling lied under oath by claiming that she was certified as Sexual Assault Nurse Examiner by the Texas Attorney General's Office (Garsee R., 2008). She had been certified as a Sexual Assault Nurse Examiner at one point, but her certification expired on April 18, 2004. As a result of Ridling's fabrication, the cases in which she gave testimony after the date that her certificate expired were re-evaluated. A child of tender years may or may not be declared a competent witness. Meanwhile, the age of a child is important but not determinative. If a young child is called as a witness, the trial judge first questions "*voir dire*." For example in *Commonwealth v Monzon* (744 N.E.2d 1131. 2001), a five-year-old child was judged competent to testify in a criminal case, but her 6-year-old sister was not because the old child did not know the difference between telling the truth and lying, whereas the younger child was able to make that distinction. Today most countries or states have statutes or court rules that enable children to appear as witnesses without specific age limitations. Also, an example of guidelines used by the court when the competency of a child witness is challenged is the test adopted by the Washington Supreme Court. In the 2011 case of *State v. Brousseau* the court affirmed the trial court's holding that a 7-year-old child was competent to testify in the rape trial of her alleged assailant. A person intoxicated by alcohol or drugs at the time of testifying will not be permitted to relate his or her knowledge in court. In some circumstances, a witness may be competent to testify regarding a particular aspect but be held incompetent to testify regarding other matters.

6.3.2 WEIGHT OF EVIDENCE

Once the evidence has been admitted into the trial, it must be weighed by the jury. The next question the court will consider is the weight that will be given to the evidence. In the case of *R v Madhub Chunder Giri Mohunt,* Birch J observed: “For weighing evidence and drawing inferences from it, there can be no canon. Each case represents its peculiarities and in each common sense and shrewdness must be brought to bear upon the facts elicited' and Lord Blackburn commented in the case of *Lord Advocate v Blantyre* that the weight of evidence depends on rules of common sense.” The object of the attorney for either side in a case is to persuade the jury to believe his or her side's view of the facts at issue and the responsibility of the defendant. The jury must then weigh all the evidence and determine which is the more believable before guilt or innocence is then determined. For example, When the computer program is not used regularly and the proponent cannot establish reliability based on its use in the ordinary course of business, the proponent may need to disclose "what operations the computer had been instructed to perform as well as the precise instruction that had been given" if the opposing party requests (*United States v. Dioguardi*, 428 F.2d 1033, 1038 [2d Cir.1970]). Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records “resulting from the operation of the computer program” affect only the weight of the evidence, not its admissibility (*United States v. Catabran*, 836 F.2d 453, 458 [9th Cir. 1988]); cited also in United *States v. Tank,* (200 F.3d 627, 630). The weight then deals with the elements of persuasion and believability. Within certain guidelines, the jury is free to give whatever weight it desires to the evidence presented to it. In essence, the entire judicial system is directed toward persuading the jury to weigh one side more favourably than the other. It has been suggested that generally, the court uses two criteria to measure the evidentiary weight of electronic records. The first is probative value: is the electronic record relevant and has authorship, authenticity, correct operation and reliability been established? The second criterion is whether, according to the rules of evidence, the electronic record has been collected and handled correctly (Dahiya and Sangwan2014). Mason with Stanfield (2016:175) point out that with respect to probative value, records must be relevant to the matter at hand and all relevant electronic records

must be presented. To meet those requirements, it must be demonstrated that the procedures used to collect electronic records were reasonable and robust enough to discover obvious, lost or hidden material.

6.3.3 BURDEN OF PROOF

The burden of proof, relevance, and admissibility are the three key concepts of evidence law. In each criminal case, the prosecution has the responsibility of affirmatively proving the allegation on which it has based its accusation and this is known as the burden of proof. Jeremy, Palmer and Roberts (2019:29) reveal that the burden of proof concept means the necessity or duty of affirmatively proving or disproving a particular fact or facts in dispute on an issue raised between the parties in a case. The burden of proof rests on the prosecution and never shifts to the defence. The defendant is never required to prove innocence, innocence is presumed and the state must prove guilt. Assuming that both the prosecution and the defence present evidence in the trial in support of their theories of the case, the prosecution must establish proof beyond, and to the exclusion of every reasonable doubt.

The jurors must be convinced that the prosecution has proved the defendant guilty beyond any doubt to which they can attach a reason (Swanson *et al,* 2019:683). Relevance on the other hand means evidence with the tendency to make the existence of a thing that is known or proved to be true and that is of consequence to the determination of the action more probable or less probable than it would be without the evidence (Swanson *et a,l* 2019:683).

6.3.4 JUDGES ROLES IN DETERMINING ADMISSIBILITY OF DIGITAL EVIDENCE

The research emerged that, in cases of common law crimes such as murder, burglary, rape or arson, because of a fairly definite state of facts, judges could know a crime was committed and can determine evidence in the case; however, in digital related crimes such as electronic fraud, distribution of child pornography, denial of service attack, identity theft, cyber-terrorism attack there is nothing known about the type of crime committed, by whom it was committed and even how it was committed. Judges have to analyse clues

to determine how the crime was committed, with some insight of knowing the legalities and technicalities before evidence is admissible.

Admissibility of evidence is a two-step process, legislative, which is a law addressing admissibility, and judicial, that is judges admit reliable evidence. In rejecting the scientific validity of the detector or polygraph, the District of Columbia Circuit Court in 1923 set forth what has since become a standard guideline for determining the judicial admissibility of scientific examination. In *Frye v. United States* 293 F. 1013 (D.C. Cir. 1923) , the court ruled that in order to be admitted as evidence at trial, the questioned procedure, technique, or principles must be generally accepted by meaningful segment of the relevant scientific community. In practice, this approach requires the proponent of a scientific test to present to the court a collection of experts who can testify that the scientific issue before the court is generally accepted by the relevant members of the scientific community. Furthermore, in determining whether a novel technique meets criteria associated with general acceptance, courts have frequently taken note of books and papers written on the subject, as well as prior judicial decisions relating to the reliability and general acceptance of the technique. The United States Federal rules of evidence offer an alternative to the *Frye* Standard and is the one that some courts believe espouses a more flexible standard for admitting scientific evidence. Rule 702 of the Federal Rules of Evidence set a different standard from general acceptance for the admissibility of expert testimony. Under this standard, a witness qualified as an expert by knowledge, skill, experience, training, or education may offer expert testimony on a scientific or technical if the testimony is based upon sufficient facts or data, the testimony is the product of reliable principles and methods, and the testimony has applied the principles and methods reliably to the facts of the case. In a landmark ruling in the 1993 case of *Daubert v. Merrell Dow Pharmaceuticals, Inc*., 509 U.S. 579 (1993) the U.S. Supreme Court asserted that general acceptance of the *Frye* standard is not an absolute prerequisite to the admissibility of scientific evidence under the Federal Rules of Evidence. According to the court, rule 702 of the rules of evidence assigns to the trail judge the task of ensuring that an expert's testimony rests on a reliable foundation and is relevant to the case.

6.4 RESEARCH QUESTION THREE (3)

- **Which problems are encountered in a digital forensic investigation relating to cybercrimes and how are these impacting the integrity of digital evidence?**

6.4.1 INTEGRITY OF DIGITAL EVIDENCE

The research established that registered tools and approved standard digital forensic laboratory is the key in digital forensic investigation to ensure integrity of digital evidence. The study revealed legal standards must be followed by virtual crime investigators in searching and seizing evidence to ensure validity and reliability of the evidence obtained. The research has illustrated that search and seizure of virtual evidence is the most important part of the investigation. It does not matter how good the analysis and procedures: if the evidence is not properly collected, it is a waste of time and resources. It became evident that when dealing with a virtual or digital crime scene it is very important to secure the scene and remove unauthorised people to prevent tampering with, or destruction of, the evidence.

The prerequisite of admissibility of digital evidence in court proceedings depends on its integrity. A former Xerox engineer, Larry Benedict, 45, was sentenced to four years in prison by a federal judge. He was accused of trafficking in child pornography. All the evidence, in this case, was electronic. Larry Benedict hired a computer expert who found evidence that pointed towards his innocence. It was found that all the evidence presented in court was allegedly tampered with or otherwise altered after it was in government custody (Electronic evidence anchors porn case - CNET, n.d.). In another case, Jodi Arias in Arizona was arrested and found guilty of the murder of Travis Alexander. She was sentenced to death. She hired a computer forensics expert to examine the victim's computer. It was found that thousands of files were deleted from the computer while it was in the custody of Mesa police department.

The problem of corruption exists worldwide and law enforcement agencies are not an exception to that. The need for protection and preservation of digital evidence during the

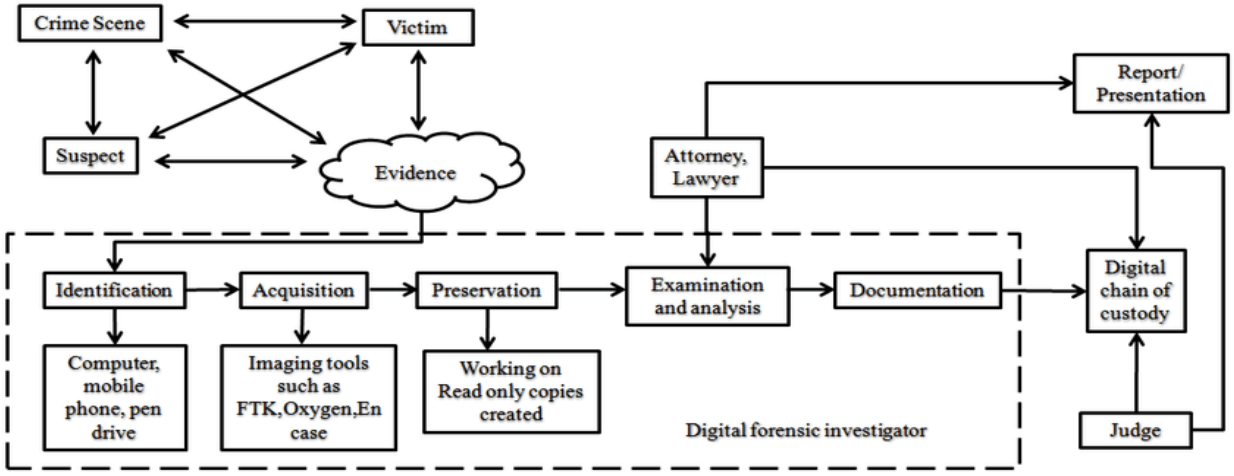
extraction phase is emphasized in the paper Saleem, Popov, and Bagilli (2014:141). It is also emphasized in the IOEC's guidelines. To minimize human interaction and subjectivity, it is important to automate the system for the preservation of digital evidence integrity and its chain of custody." Digital evidence is fragile in nature and it is handled differently.

6.4.2 CHAIN OF CUSTODY

The research emerged that digital evidence is considered as valid if the chain of custody can demonstrate where, when and who came into contact with the evidence in each stage during the investigation process. It emerged in this study that to use digital evidence in a criminal or civil trial, the party offering the evidence has the burden of providing that the evidence is genuine and authentic. This requires testimony establishing an adequate foundation about where and how the data was obtained and that the data offered in evidence is the data that is claimed to be. The chain of custody is the witnessed, unbroken, written chronological history of who had the evidence from the time it was received, through and including all other possessions (Swason, *et al* 2019:57). Casey (2011:21) state that one of the most important aspects of authentication is maintaining and documenting the chain of custody of evidence. A chain of custody is an important principle in investigation and concerns the handling of evidence and its integrity (Marcella *et al*, 2012:12). Each person who handled evidence may be required to testify that the evidence presented in court is the same as when it was processed during the investigation. The party leading the evidence in court must always prove the location, date, and time of collection and demonstrate that the evidence has not been altered since collection. A chain of custody is therefore considered necessary to demonstrate the admissibility of evidence (Bergman and Sara, 2005:400). Although it may not be necessary to produce at trail every individual who handled the evidence, it is best to keep the number to a minimum and maintain documentation to demonstrate that digital evidence has not been altered since it was collected (Casey, 2011:57).

"In other for digital evidence to be useful in exonerating the innocent and pursuing suspects it must be treated in accordance with its importance. The evidence must be located, its position documented, collected, be identified marks and writing on it and or

on the package in which it is placed, and be transmitted to the evidence room or the crime laboratory. The electronic evidence admissibility at trial court might depend on whether the chain of custody has not been altered. Smith, Mann and Urbas (2018:20) caution that, in court, the defence capitalises on challenging the integrity of evidence. According to the authors, the interest of the defence is in raising doubts and confusion about the evidence assembled and presented in court by the prosecution." The diagram below shows the movement of evidence from the crime scene to the judge in court.



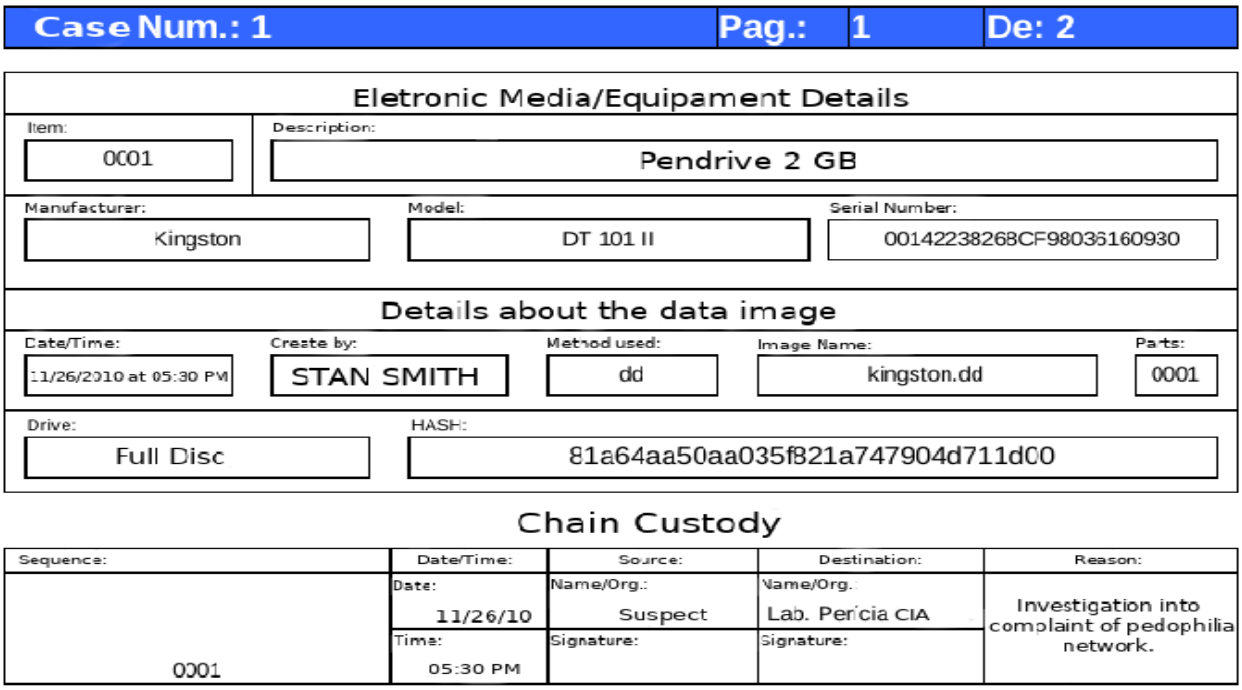
- Figure 6.1 Depict the Movement of Digital Evidence. Source: Rana et al (2017).

6.4.2.1 Chain of custody form

The research established that chain of custody form must be used by digital forensic investigators and law enforcement in investigation process. The chain of custody form lists all or any seized evidence in sequence and is noted in the same fashion as the identifying marks on the packaging. At the bottom of the form is a place for the signature of the person who collected the evidence and turned it over to the next person, who then is in charge of the material.

It basically forms a branching tree so the origin of the crime or from the body. If at any point the chain is broken, the evidence can become inadmissible to court and useless. A

sample chain of custody form is shown in figure 6.2 recording the transfer of evidence, when, where, and why.



Case Num.: 1	Pag.:	1	De: 2

Eletronic Media/Equipament Details

Item:	Description:		
0001	Pendrive 2 GB		
Manufacturer:	**Model:**	**Serial Number:**	
Kingston	DT 101 II	00142238268CF98036160930	

Details about the data image

Date/Time:	Create by:	Method used:	Image Name:	Parts:
11/26/2010 at 05:30 PM	STAN SMITH	dd	kingston.dd	0001
Drive:	**HASH:**			
Full Disc	81a64aa50aa035f821a747904d711d00			

Chain Custody

Sequence:	Date/Time:	Source:	Destination:	Reason:
0001	Date: 11/26/10	Name/Org.: Suspect	Name/Org.: Lab. Perícia CIA	Investigation into complaint of pedophilia network.
	Time: 05:30 PM	Signature:	Signature:	

- Figure 6.2 An example of a filled chain of custody form. Source: Almeida et al (2019). Computer forensic.

6.4.3 ANALYSIS AND AUTHENTICATION OF DIGITAL EVIDENCE

The research established that virtual evidence or digital evidence analysis is vital to the success of any criminal investigation. The research show that the utmost concern is due to the volatile nature of digital evidence. The research that virtual evidence or digital evidence analysis is the process of examining or evaluating information and during this process, the investigator examines the history of the information; for example, who edited or accessed the information, and determines whether electronic evidence was tampered with.

Another point of great importance found the research is that, in order to preserve the original evidence a duplicate copy should be used for analysis. The research emerged that law enforcement or investigator should bear in mind that when analysing evidence the process can lead to uncovering sources of new evidence. In light of the above, the investigators should consider using special analysis tools to analyse the evidence seized. These tools help with the visualisation of the evidence in a form of flow and link analysis charts, as observed by Casey (2011:185). Evidence authentication may also clearly show errors in question and will not have an adverse effect on the evidence itself. For instance, in *DPP v McKeown* [1997] UK HL JO220-1*; DPP v Jones,* the clocks on the Intoximeter 3000 used to measure the breath alcohol values of the defendants were not accurate. For this reason, the defendants challenged the admissibility of the print-outs from the device. In addressing whether the accuracy of the clocks was relevant to the accuracy of the print-out readings, Lord Hoffmann examined the functioning of these devices and concluded that, for the purposes of Section (6)9 of the Police and Criminal Evidence Act 1984, a malfunction was irrelevant unless it affected the way in which the computer processes, stores or retrieves the information used to generate the statement. On the facts, the clock was not part of the processing mechanism of the Intoximeter, and the convictions of the defendants based on the print-out readings were upheld (*DPP v McKeown DPP v Jones; DPP v Jones).*

Casey (2011:61) is of opinion that courts generally ask if the recovered evidence is the same as the originally seized data when considering whether digital evidence is admissible. As indicated, the authentication of digital evidence involves validation and extraction of the evidence from a computer system to ensure that it is as legitimate as the original and authentication relate to the question of whether the document is what it claims to be. In court proceedings, an adjudicator will be required to determine the credibility or reliability of the evidence presented and tested in court. This accentuates the fact that the investigator must be able to coax or persuade the court that the evidence was derived from the computer at the crime scene. For instance, the investigator may use information about system security access to the computer files as proof that the evidence has not been tampered with whilst in the computer system mentioned by (Casey 2011). Once the evidence has been authenticated, the investigator must perform an analysis of the

collected evidence. Casey (2011:57) demonstrates that digital evidence is authentic if it is generally necessary to satisfy the court that it was acquired from a specific computer and/ or location, that a complete and accurate copy of digital evidence was acquired, and that it has remained unchanged since it was collected. In some cases, it may also be necessary to demonstrate that specific information is accurate, such as dates associated with a particular file that is important to the case.

6.5 RESEARCH QUESTION FOUR 4:

- **What are the key national legislative framework and Ghana's regional and international obligations to combat Virtual crime or Cybercrime to what extent, and based on which anti-cybercrime strategies, has other countries effectively been able to combat cybercrimes?**

6.5.1 CYBER SECURITY FRAMEWORK IN GHANA AND INTERNATIONAL LEGAL FRAMEWORK ON CYBERCRIME INVESTIGATIONS AND ELECTRONIC EVIDENCE

The research found that there are key national and international legislative framework and stardards to combat virtual crime or cybercrime but investigators lack the skills and are faced with challenges of searching and seizing digital evidence or executing search warrant outside their jurisdiction as they are not equipped to address extraterritorialities of digital crime. It was also emerged that lack of uniformity in the cybercrime laws make it difficult for investigators to initiate investigation or conduct investigation in other jurisdiction. The research established that there are no common approaches to fighting cybercrime. Instead, there have been several suggestions on how to institute a uniform legal code for cybercrime investigations in the united nation. As proved in this study, most cases of cybercrime are transnational in nature, only a broad international consensus and a global joint effort on the criminalisation of cybercriminals' actions in all of their forms, which is implemented through the exercise of universal jurisdiction of international courts can, bring cybercriminals to justice. Although the research found that many legal frameworks and treaties exist, none of them provides a binding regulatory jurisdiction. The research has shown that the United States promote security cyber activities and try to prevent and combat cyber-related crime at the international level and also emerged in

this study that the Council of Europe Convention or the Budapest Convention on Cybercrime is the most important treaty in fighting against cybercrime at the international level.

The rapid increase in many different, advanced and worldwide threats to information security, in amalgamation with the compliance requirement of a flood of computers and privacy-related regulations around the world, is being blown by organisations to take an extra tactical view of information security. It looks right on that hardware, software or vendor-specific solutions to organization and individual information security challenges are on their own dangerously and inadequate. While the greatest number of co-operations or companies believes that their information systems are secure, the vicious truth is that they are not. Not only is it exceptionally difficult for a co-operation to operate in today's world without effective information security, but such cooperation has become a threat to their more answerable compatriot. The extent and value of electronic data are continuing to grow exponentially and the vulnerabilities of businesses and individuals to data misappropriation or destruction are also growing very quickly. Fundamentally, consumers' top secret in dealing with the electronic environment depends on how secure they believe personal data are stored. Cyber security, for this reason, matters to any jurisdiction, co-operations with any form of virtual or cyber strategy from simple business–to–consumer (B2C) or business–to–business (B2B) propositions through enterprise resource planning (ERP) systems to the use of extranets and email. It matters, too, to any co-operation or businesses that rely on information and communication technologies for its day-to-day operations or that may be imperiled to the provision of data protection and cyber security legislation.

6.5.2 CYBERCRIME LEGISLATIONS IN GHANA

In Ghana today, the activities of cyber criminals have become a threat to society. "The preponderance of cybercrime involving "Sakawa" as popular termed in Ghana and involving phishing, money laundering, advanced fees fraud, child pornography, and mobile money fraud to mention a few has had a severe negative impact on Ghana's image including decreased foreign Direct investments in the country. With the arrival of the information age, legislatures have been struggling to redefine laws that fit crimes

committed by criminals. Initially, there were no specific laws in Ghana for combating cybercrime. This led to the creation of an ideal environment for criminals to operate without any law to combat their criminal activists. The menace of cybercrime and the magnitude and gravity of the situation led to the passing into law such as the, Electronic Communication Act 775 of 2008, National Information Technology Agency Act 71 of 2008, Data Protection Act 843 of 2012**,** Electronic Transaction Act 772 of 2008, and Ghana's Cybersecurity Act 1038 of 2020 which provides for the prohibition, prevention, detention, response and prosecution of cybercrime and other related computer crime matters.

6.5.2.1 Electronic Transaction Act of 772 of 2008

In December 2008 Parliament of Ghana enacted the Electronic Transaction Bill into law (2008 Parliament of Ghana, 2008). The primary objective of the Act is to secure cyberspace as a means of mitigating crime incidence that may affect the ability of citizens to create worth. There are twelve groups of clauses in the Act. These are electronic transactions, electronic government services, the certifying agency, consumer protection, protected computers and critical database, Domain name registry, and appeal tribunal. Other clauses relate to the industry forum, the liability of service providers and intermediaries, cyber inspectors, cyber offences, and miscellaneous matters. Law enforcement is dealt with in the tenth group of the clauses and the Act empowers security agencies in the course of the execution of court warrants to seize a computer, electronic record, programme, information document or thing if they reasonably believe that an offence has been or is about to be committed." However, the scope of the enforcement of the Act is limited by the area of jurisdiction as it's contained in clause 142 (2): This Act applies if, for the offence in question:

(a) The accused was in the country at the material time;
(b) The electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time;
(c) The electronic payment medium was issued by a financial institution in the country

(d) The offence occurred within the country, on board in Ghanaian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence was committed, whether paragraph (a), (b) or (c) applies.

Law enforcement agencies may also request the preservation of evidence by providers of wire or electronic communication services or a remote computing service pending the issuance of a Court Order, clause “(Electronic Transaction Act 772 of 2008 clause100)”. The Courts is empowered, upon application of a law enforcement agency, to order an electronic communication service provider to disclose the contents of an electronic communication, that is in transit, held, maintained or that has been in electronic storage in an electronic communications system if the disclosure is relevant for the investigative purposes in the interest of national security, clause (Electronic Transaction Act 772 of 2008 clause 101).

The ETA 2008 has specific legislation on cybercrime and prescribes punishment for cybercrime perpetrators. The Act addresses issues in the fight against cybercrime. Pillar 14 and the ETA fail to capture a holistic approach to securing cyberspace as a means of mitigating cyber incidences that may affect the ability of citizens to create wealth. The provisions on electronic transactions are based on the UNICTRAL Model Law of 1996, as well as elements of the United Nations Convention on the Use of Electronic Communications in International Contracts (2005). Sections 98-106 address issues of criminal procedure in cybercrime investigations, while sections 107-140 establish cyber offences. The powers granted to so-called 'Cyber inspectors that is persons from the NITA or any other agency enforcing the provisions of the ETA, are in addition to any traditional powers given to law enforcement agencies under the Criminal Procedure Code 1960 (Act 30). For example, a 'cyber inspector' can request the assistance of a third party, such as an IT expert, in the course of an investigation. In addition, requests may be made to certain service providers to preserve electronic records that may be required as evidence, which would be subsequently disclosed in response to a valid court order. Service providers are also required to retain logs and records concerning the use of their services. The ETA modifies the Criminal Offences Act 1960 in respect of some forms of criminal conduct, such as 'stealing', 'appropriation' and 'representation', in order to enable these

traditional provisions to be used against similar conduct occurring within a cyberspace environment. New offences are also established under the ETA to address conduct aimed at undermining the integrity of computer systems, such as unauthorized access, interception and interference. The third category of offences relates to the distribution of illegal content, specifically child pornography.

Traditionally, legal jurisdiction involves territories with the scope of a country being defined by the limit of its boundaries. This territorial notion is ineffective to prosecute cybercriminals. Determining where cybercrime is committed can be difficult since the perpetrators and the victim can be located in different countries. The offenders may also utilize computer systems in different countries to attack their victims. Another pitfall of the Act is that punishment is not clearly stated as in the drug trafficking law and this allows judges to exercise their discretional powers to make a pronouncement on cyber offences. For instance, under the Narcotics Drugs Law (P. N. D. C. L 236), Section 2(2) states that "a person found guilty of a narcotic offence is liable on conviction to a term of imprisonment of not less than ten years". Additionally, properties acquired by scammers by fraudulent means are not seized or confiscated unlike the Drugs Law, Section 11 to 14 which stipulated that properties acquired by drug traffickers should be seized. This law provides a vent for the criminal as the weight of the punishment does not commensurable with the nature of the cybercrime. Therefore, it is not surprising that the Ministry of Communications in 2014 concluded in their final draft report on Cyber Security Policy that even though the ETA has provisions for law enforcers to fight against cybercrime, however, this is not adequate and does not address fully all aspects of cyber security, especially the multi-stakeholders approach.

6.5.2.2 Electronic Communication Act 775 of 2008

Today, the mantra of telecommunication or electronic communication policy is to promote the public interest through the promotion of vigorous competition in all markets for telecommunications services and between all modes of service delivery, with consumer safeguards where appropriate. In 2008, the Ghana government instituted Electronic Communication Act, 2008 (Act775) which serves as a central body to license and regulate

communications activities and services in the country and to provide for related purposes. The sections in the Act include licenses and frequency and authorization, broadcasting service, application, interconnection, access to facilities and international transmission capacity, universal service, universal code and tariffs, consumer protection, Ghana investment fund for electronic communications, rural communications services, spectrum management, road works and access to land, the national electronic communication numbering plan, terminal equipment and technical standards, testing and inspection, enforcement power of the authority, offences, fees, resolution of disputes, electronic communication Tribunal, and general provisions.

Section 73 (1) of the Electronic communication Act (775) states that a person who knowingly obstructs or interferes with the sending, transmission, delivery or reception of communication, steal a transmitted message or data, intercepts or procures another person to intercept, without the authorization of the provider or user, or court order, or otherwise obtains or procures another person to obtain, unlawful access to communication transmitted over electronic communication network commits an offence and is liable on summary conviction to a fine of not more than three thousand penalty units or a term of imprisonment of not more than five years or both. Section 76 (1) also emphasises false communication and states that a person who by means of electronic communication service, knowingly sends a communication which is false or misleading and likely to prejudice the efficiency of life-saving service or to endanger the safety of any person, ship, aircraft, vessel or vehicle commits an offence and is liable on summary conviction to a fine of not more than three thousand penalty units or a term of imprisonment of not more than five years or both.

6.5.2.3 National Information Technology Agency Act 771 of 2008

National Information Technology Agency Act 771 of 2008, promotes private sector partnership in ICT deployment, ensures the security of networks at all times, advises the ministry on policy review in the ICT sector and investigate, resolve disputes between license holders under the electronic transactions act referred to the agency by license holders and to certify all agencies established under the electronic transactions act, 2008 (act 772). The Act enhances to Maintain registers for approval given for equipment used under the Electronic Transaction Act, 2008 (772) and establishes the quality of service indicators and reporting requirements that apply to the license holders under the Electronic Transaction Act, 2008 (772). It's interesting to note that fake websites are being created every day by internet hackers and duped innocent people without NITA detection or apprehension. This could be attributed to the inadequate skilled manpower or technical enabling environment to track the perpetrators.

6.5.2.4 Data Protection Act 843 of 2012

The Data Protection Act 843 of 2012 is one of the key legislations to improve legal certainty and transparency in cyberspace. The Data Protection Act 843 of 2012 was passed by parliament in 2012, to protect the privacy of individual and personal data. The Minister of Communications on Thursday, November 18th, 2014 inaugurated an 11-member governing board of the Data Protection Commission (DPC) chaired by the Supreme Court Judge, Justice Date-Bah to regulate the processing of personal information on the internet.

The Commission has the power under section 3 of the Act to:

(a) Implement and monitor compliance by individuals who utilize the electronic industry
(b) Make the administrative arrangements it considers appropriate for the discharge of its duties;
(c) Investigate any complaint under this Act and determine it in the manner the Commission considers fair; and
(d) Keep and maintain the Data Protection Register.

Privacy fortified human dignity and guaranteed other key rights such as freedom of association, and speech as enshrined under Article 18(2) of the 1992 Constitution of Ghana. The information and communication technologies are being used by numerous anti-social elements in aiding their illegal activities. Explained that data in the wrong hands have caused untimely death and jeopardized many lives. Therefore, it is imperative that strong provisions are made to protect people against the abuse by those institutions that keep their information on the internet such as schools, hospitals and governmental organizations. The intended purposes of the Data Protection Commission are yet to be fulfilled because data are still collating from the various institutions which controlled individuals' information online.

6.5.2.5 Criminal Offences Act 29 of 1960

The growing Internet penetration in Ghana had opened up the country to new online trading platforms, which had empowered the average Ghanaian to transact various business operations. Even though the online portal serves as a medium of exchange for goods and services, most transactions take place offline. As a result, some Sections of the Criminal Offences Act (29/30) are recaptured in the Electronic Transactions Act (Act 772) to prefer charges against cybercrime suspects. These Sections include: 20, 21, 23, 122, 124, 133, 137, and many others. Crimes committed under these Sections of the Criminal Offences Act 29/60 which have been reiterated in the Electronic Transactions Act (Act 772) are bailable offences and carry lesser punishment which cannot deter fraudsters from committing such offences. Besides, Danquah and Longe were of the view that the criminal code under which cybercrime suspects are currently charged has existed under the fraud laws established in 1960 which gives room for defence lawyers to often win and acquit their client because some of the facts do not support the prosecutor's evidential claims.

6.5.2.6 Ghana’s Cybersecurity Act 1038 of 2020

In December 2020 Parliament of Ghana enacted Ghana's Cybersecurity Act 1038 of 2020 into law. It is a 68-page document made up of 100 sections and 3 schedules. The sections are grouped into 18 different subject headings. This Act has become necessary because of the rapid digitalization of the Ghanaian economy, coupled with the high rate of cyber-crimes and other cybersecurity incidents in the country. The primary objective of the Act is to promote the development of cybersecurity and regulation of cybersecurity activities in Ghana. The Cybersecurity Act, 2020 Act focuses on the protection of Ghana's Critical Information Infrastructure. The Act empowers law enforcement to prevent management and respond to cybersecurity threats and cybersecurity incidents. Sections 35 to 40 of the Cybersecurity Act, 2020 seek to protect Ghana's Critical Information Infrastructure with provisions for Designation, Registration, Withdrawal of Designation, Management and Compliance Audit of Critical Information Infrastructure and access it as well.

The Act is applicable to all activities involving cybersecurity in Ghana and the establishment of the Cyber Security Authority (Authority) as a corporate institution or body. The Act empowers the government to establish an 11-member board that governs the Cyber Security Authority. The Act also establishes a Joint Cybersecurity Committee made up of 18 members across different ministries, departments, and agencies. The Authority is headed by a Director-General, who is appointed by the President. The Act establishes national and sectoral computer emergency response teams (CERT) and these institutions are compelled or obliged to report cybersecurity incidents to the relevant sectoral or national CERT within 24 hours after detecting the incident. Per the Cybersecurity Act, 2020 (Act 1038), providers of the cybersecurity service can only operate upon obtaining a license from the Cyber Security Authority and revocation of the license can be done by the same Authority based on the defined conditions of the Cyber Security Act.

6.5.3 CYBERCRIME: THE GLOBAL TREND AND STATISTICAL INDICATORS

The research found that nothing remains static within the world of technology, and cyber security is no different. It was established that all around the world, developers and engineers at technology companies or in Information Technology security departments of other businesses continually work on methods to safeguard valuable personal, financial and professional data. The research established that a data infographic compiled by cyber security solutions firms RSA noted that in every twenty (20) malware attacks around the globe involves the use of ransomware. As established in this study, according to cybersecurity ventures (2021), the cost of cybercrime globally is expected to grow by 15 percent per year over the next five-year period and it will reach $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. Ransomware attack and damages report by cybersecurity Ventures in 2017 predicted the cost and damages of ransomware to be $5 billion up from $325 million in 2015, a fifteen percent increase in just two years. In 2018 the damages were estimated at $8 billion, then raised to $11.5 billion in 2019, and in 2021 the forecast for global ransomware damages and cost hit $20 billion which is a fifty-seven percent increase more than it was in 2015. Destruction of data, stolen money, theft of intellectual property, theft of personal and financial data, fraud, post-attack disruptions to the normal course of business and restoration and deletion of hacked data and systems are among the cost of cybercrime globally.

The research found that ransomware has evolved and expanded dramatically in the interim and all signs are that the coming decade will be even worse as ransomware gangs are increasing exponentially and continue to refine and intensify their attacks. It is estimated that ransomware will cost its victims more than $265 billion (USD) annually by 2031 (Cybersecurity Ventures, 2021). The global cybersecurity market was worth $120 billion in 2017. The study has shown that global spending by industries on cybersecurity products and services for defending against cybercrime was projected to exceed $1 trillion cumulatively over the five years from 2017 to 2021(Cybersecurity Ventures, 2021). In 2018 the United States Federal Bureau of Investigation (FBI) as a supervisory special agent to US government investigates cyber intrusion and told the Wall Street Journal that every American citizen should expect that all of their data has been stolen through the

dark web, which is an internationally hidden electronic environment used to conceal and promote heinous crime on the cyber world. Furthermore, the dark web is an electronic environment where virtual criminals conduct business-to-consumer activities or purchase and sell venerable software such as malware, exploit kits, and internet attack services to strike cyber victims including co-operations, utilities, and governmental institutions.

Globally, healthcare industries lagged behind other industries such as banking and financial institutions, law enforcement agencies, insurance industries, and educational institutions. The global cybercrime target on healthcare industries is because of the outdated computer technology systems and fewer protocols and Information Technology staff used and the payment of the quick ransom they make to regain data.

Augenbaum (2021) posits that small and medium-sized businesses lack the financial resources and skill set to combat the emerging cyber threat. The global concerns on cybercrimes are ransomware attacks and small businesses have taken huge concern since the cost of ransomware has skyrocketed and it does not look like it will end today or tomorrow. World Wide Web criminals are investing in more advanced and innovative scams to lunch massively destructive attacks to cause huge collateral damages. There has been an upward trend on the scope and material cost of cybercrime some Europe member States now report that the recording of cybercrime offences may have surpassed those associated with traditional crimes. Data breaches among cooperation have been common in the last decade due to the rapid increase use of digital or electronic files and reliance on cyber data by my institutions. For example, between 2013 and 2016 over three (3) billion yahoo user accounts were exposed and it was one of the worst and most infamous cases of cyberattack. The attackers uses backdoor stolen backups, and access cookies to steal user records including personal identifiable information such as name, date of birth, mobile number, addresses and others. Furthermore, in 2021 Facebook suffered a major cyber-attack where over 530 million users accounts were exposed and Microsoft also suffered a major attack in 2021 where 30000 US companies and 60 000 companies worldwide were affected by the sweeping attack on the Microsoft Exchange email server. Whether the cyber-attack is intentional or not, 60% of data breaches occur through the actions of an insider or current employee or former employee.

6.5.3.1 The International Challenges and Response towards fighting Cybercrime

The research found that the ever-growing use of computers and information communication technologies in the world of "e-everything" has opened up a range of new activities for crime to take place through electronic means on a global scale, irrespective of national and transnational borders. It was discovered in the study that there should be cooperation among countries because cybercriminals are not confined by national or geographic boundaries and electronic evidence relating to a single crime can be dispersed across multiple regions. The effective combating, investigation and prosecution of such crimes require international cooperation between countries, law enforcement agencies and institutions backed by laws, international relations, conventions, directives and recommendations culminating in a set of international guidelines to fight cybercrime (Ana et al, 2012:23). The increasing incidents of cyber-attacks against sovereign states and their critical information infrastructures necessitate a global response. Regional and bilateral agreements and local legislation are not sufficient to deter cyber-attacks (Pardis et al, 2016). Regional and bilateral agreements and local legislation are not sufficient to deter cyber-attacks. Therefore, international law is a necessary tool to enable the global community to deter cyber threats in its various jurisdictions (Pardis et al, 2016). Although there are many challenges to international cooperation and the establishment of international guidelines to fight global cybercrimes across borders, there is a prerequisite for the harmonisation of countries' criminal laws, the sanction of complex jurisdictional issues and the development of new cooperation procedures to challenge cybercrime, its extent and location (Goodman, as cited in ITU Report 2009). It is necessary to identify the perpetrators across borders anywhere in the world, and to investigate and to secure electronic evidence of their crimes so that they may be brought to justice in any compliant jurisdiction with fairness and compliance with human rights standards. Among the challenges faced by law enforcement agencies is the lack of harmonisation of national criminal laws regarding cybercrimes and the difficulties to find a clear and comprehensive definition of computer-related crime. Growing reliance on ICTs makes systems and services more vulnerable to attacks against critical Infrastructures.

With the increasing number of internet users, the growing number of people connected to the Internet, the number of targets and offenders increases and there are also complex jurisdictional issues to confront, given the multiplicity of countries potentially involved in cybercrime.Law enforcement typically stops at the borders of nations or states and must go through proper legal channels and procedures to receive assistance in pursuing cybercrime investigations and prosecutions. It also becomes necessary to seek the assistance and support of agencies such as Interpol, Europol, and FBI some certified agencies to not only help in the investigations and prosecution processes but also extradition of criminals from one jurisdiction to another. These processes require a complex set of different skill levels for cybercrime investigations, forensic analysis, custody of the evidence, prosecution and extradition within a country, between countries and agencies to be efficient and effective. Support assistance is also required to accommodate different jurisdictions' legal systems and procedures. Foreign or external assistance may be needed even if the act is local within a country because the criminal activity transcends the e-world of signals, codes, wires and machines across one or more transnational borders. At first glance, the worldwide legislation regarding cybercrime seems to be somewhat of a mess. There are numerous international approaches and coalitions around the world all attempting to create a stable online environment both domestically and internationally. The lead international bodies are the United Nations, the G-8 Subgroup on High-Tech Crime, the Organization for Economic Cooperation and Development and the Council of Europe.

6.5.4. THE INTERNATIONAL CONVENTION AND DIRECTIVE ON COMBATING CYBERCRIME

The transactional and borderless character of modern information systems means that attacks against such systems are often trans-border in nature, thus underlining the urgent need for further action to approximate criminal laws in this area. The following are the international conventions an directives on combating virtual crime or cybercrime:

6.5.4.1. Council of Europe Convention on Cybercrime: Budapest Convention

The Council of Europe was established in 1949 primarily as a forum to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe. Based in Strasbourg, its work and programme include legal cooperation, social and economic questions, health, education and culture. It provides a forum for both EU and non-EU nations to agree on harmonising conventions. Some nations from outside Europe have been admitted as observers to the Council, including Canada, Japan and the U.S. Since the late 1980s, the Council of Europe (CoP) has been working to address the growing international concern over the threats posed by hacking and other computer-related crimes. In 1989, the Council published a study and recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks (Recommendation No. R. (89) 9, which was adopted by the Council on 13 September 1989). This document "recommends the Governments of member states to take into account when reviewing their legislation or initiating new legislation, the report on computer-related crime and in particular the guidelines for the national legislatures.

The Budapest Convention on Cybercrime was the first international treaty to address Internet and computer crime through the harmonisation of national laws, improving investigative techniques, and increasing cooperation among nations (Budapest Convention on Cybercrime, 2001). It is also the first on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation (Budapest Convention on Cybercrime, 2001). The cybercrime convention is an agreement between states. The parties to the convention must criminalize certain cybercrimes in their national substantive criminal law. Article two (2) of the COE convention aims at criminalizing offences that compromise the confidentiality (Budapest Convention on Cybercrime,

2001), integrity and availability of computer data and systems. In particular, chapter two (2) articulates that each party must establish as a criminal offence under its domestic laws when committed intentionally, measures to be taken at the national level regarding substantive criminal law. This consist of (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) Computer-related offences; (3) Content-related offences; and (4) Offences related to the infringement of copyright and related right, ancillary liability and sanctions (Budapest Convention on Cybercrime, 2001).

The European Union (EU) Framework Decision is an effort to bring some consistency in the area of justice and home affairs including computer crime. The European Union (EU) adopted Framework Decision 2005/222/JHA on attacks against information systems on February 24, 2005, with an objective to improve cooperation between judicial and other competent authorities, including the police and other specialized law enforcement services of the member states, through approximating rules on criminal law in the member states in the area of attacks against information systems. It is recited in the preamble to the Framework Decision that criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems and to contribute to the fight against organized crime and terrorism and that significant gaps and differences in member states' law in this area may hamper the fight against organized crime terrorism.

In the area of computer-assisted crime and content-related crimes, the EU Council adopted Framework Decision 2001/413/JHA on combating fraud and countering non-cash means of payment, which includes offences related to computers and offences related to specifically adapted devices which came into force on June 2, 2001, and adopted Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography which recognizes that child pornography is increasing and spreading through the use of new technologies including the Internet (European Parliament, 2005).

6.5.4.2. United Nations Convention on Cybercrime and Cybersecurity

In 1990, the eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders approved a resolution in which it requested to the Member States to increase their efforts to fight computer-related crimes by considering, if necessary, the following measures: modernization of national criminal laws and procedures; improvement of computer security and prevention measures; adoption of adequate training measures; and elaboration of rules of ethics in the use of computers (Ana *et al* 2007). The eighth UN Congress also recommended in this resolution that the United Nations Committee on Crime Prevention and Control "should promote international efforts in the development and dissemination of a comprehensive framework of guidelines and standards that would assist Member states in dealing with computer-related crime and that it should initiate and develop further research and analysis in order to find new ways in which member states may deal with this problem in the future (Piragoff, 2000). In 1994, the U.N published the United Nations Manual on the Prevention and Control of Computer-Related Crime (United Nations, 1994). This Manual studied the phenomenon of computer-related crimes, substantive criminal law protecting privacy, procedural law, and the needs and avenues for international cooperation “(Ana *et al* 2007)." Finally, a Resolution on combating the criminal misuse of information technologies were adopted by the General Assembly on December 4, 2000 (A/res/55/63), that included: "(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies. (d) Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized (Ana et al, 2007).

6.5.4.3 Commonwealth of Australia Cooperation Directive on Cybercrime

The internet and digital economy represent a significant opportunity for Australia (Australia Government, 2022). However, cyber criminals increasingly exploit Australia's digital connectivity for their criminal activities (Australia Government, 2022). In 2022, the Australia Government issued a National Plan to Combat Cybercrime that builds on the

2013 Plan to formalise a framework that focuses on three key pillars: Prevent and Protect; Investigate, Disrupt and prosecute; and Recover (Australia Government National Plan to Combat Cybercrime, 2022). The impact of cybercrime on Australia's society and economy is so significant that a national response is imperative (Australia Government National Plan to Combat Cybercrime, 2022). The Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report from 1 July 2020 to 30 June 2021 highlighted that self-reported losses due to cybercrime totalled more than AU$33 billion during the 2020–21 financial year (Australian Cyber Security Centre Report, 2020). Australia has a strong criminal offence and law enforcement framework to address a broad range of cybercrimes (Australia Attorney-General's Department, 2020). This includes a comprehensive set of computer and telecommunications offences under Parts 7.3, 10.6 and 10.7 of the Commonwealth *Criminal Code Act 1995*. They include (Australia Attorney-General's Department, 2020):

- dishonestly obtaining or dealing in personal financial information .
- online child sexual exploitation and abuse
- cyber abuse including non-consensual sharing of intimate images
- computer intrusions
- unauthorised modification of data, including destruction of data
- unauthorised impairment of electronic communications, including denial of service attacks
- the creation and distribution of malicious software (for example, viruses and ransomware)

Each state and territory in Australia has its own cybercrime related offences that complement Commonwealth legislation as well as legislation which covers online fraud and other technology enabled crimes (Australia Attorney-General's Department, 2020). The Commonwealth has enacted a comprehensive set of offences to address cybercrime, contained in the *Criminal Code Act 1995* (Criminal Code). These offences are based on model laws agreed to by Commonwealth, state and territory governments in 2001. The offences are consistent with those required by the Council of Europe Convention on Cybercrime and are drafted in technology-neutral terms to accommodate advances in

technology (Australia Attorney-General's Department, 2020). Key Commonwealth offences are contained in Part 10.6 and Part 10.7 of the Criminal Code, which contains offences criminalising the misuse of telecommunication networks, ‘carriage services’ (a term which includes the internet and online services, wired and mobile services and computers (Australia Attorney-General's Department,2020). The Commonwealth computer offences are complemented by state and territory laws which criminalise the misuse of data and computer systems (Australia Attorney-General's Department,2020).

6.5.4.4 Africa Union Convention on Cybersecurity and Data Protection

In 2014 African Union (AU) adopted a credible legal framework for cyber security and data protection which addresses in particular, the need for cyber legislation on the African continent. According to Snail (2016), the AU convention seeks to harmonise African cyber legislation on electronic commerce, personal data protection, cyber security promotion and cybercrime control. Chapter three (3) of the AU convention makes provision for promoting cyber security and combating cybercrime. Article 24 of chapter (3) of the framework emphasises each State undertakes to develop, in collaboration with stakeholders, a national cyber security policy which recognizes the importance of critical information infrastructure for the nation and identifies the risks facing the nation in using the all-hazards approach and outlines how the objectives of such policy are to be achieved “(Africa Union Convention on Cybersecurity and Data Protection. 2014)”. Article 25 of chapter (3) of the framework allows each party state to adopt such legislative and or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders. In adopting legal measures in the area of cyber security and establishing the framework for implementation thereof, each State Party shall ensure that the measures so adopted will not infringe on the rights of citizens guaranteed under the national constitution and internal laws, and protected by international conventions, particularly the African Charter on Human and Peoples' Rights, and other basic rights

such as freedom of expression, the right to privacy and the right to a fair hearing, among others.

In addition, the Africa Union Convention on Cybersecurity and Data Protection (2014) differentiates and proposes amendments to existing laws such as offences specific to information and communication technologies, offences relation to electronic message security measures, proposes adapting certain information and communication technologies offences and proposes adapting certain sanctions to the information and communication technologies. From the above-mentioned aspects, purposes and objectives of the discussion on the Africa Union Convention on Cybersecurity and Data, one can clearly and easily identify the same objective and purpose for the basis of the Electronic Transaction Act. This is evidenced in the COE convention where member states are obliged to: criminalize the illegal access to computer systems, illegal interception of data to a computer system and interfering with computer systems without right and intentional interference with computer data without right." What is more, the objectives can purpose of the ECT Act introduces the criminalization of the above aspects mentioned under the COE Convention.

6.5.4.5 United States of America (USA) Directive on Cybersecurity and Cybercrime

Internationally, countries have enacted legislation to deal with cybercrime and the problems associated therewith. The US has a well–documented history of applicable policy and law that provides a road map for national cyber security (White House, 2009). The first security and economic policy frameworks for securing cyberspace emerged in 1998 and were the result of Presidential Decision Directive (PDD) 63 on "Critical Infrastructure Protection" and the Department of Commerce's Green Paper (White House, 2009).

Presidential Decision Directive (PDD) 63 was later updated and codified in 2003 as the "National Strategy to Secure Cyberspace" and the Homeland Security Presidential Directive (HSPD) 7 on "Critical Infrastructure Identification, Prioritization, and Protection,"

both of which prioritized a cyber-space threat reduction program. (Presidential Decision Directive, 2003). That same year the Department of Homeland Security was created and tasked with coordinating a cross-agency response to national cyber threats.(Presidential Decision Directive, 2003).

The Federal Bureau of Investigation (FB1) and the United States Secret Service (USSS) play prominent roles in investigating computer-assisted and cybercrimes. The FBI has a four-fold mission in this area namely (Federal Bureau of Investigation, 2008):

(a) To stop those behind the most serious computer intrusions and the spread of malware
(b) To identify and thwart online sexual predators who use the Internet to meet and exploit children and those who produce, possess, or share child pornography
(c) To counteract cooperation that targets U.S. intellectual property endangers national security or competitiveness and
(d) To dismantle national and transnational organized criminal enterprises engaging in Internet fraud.

The FBI Operational Technology Division (OTD) provides a number of tools that are used to analyse digital data and computer systems in large-scale hacking and cybercrime cases. These same tools can be used to address cyber-espionage cases, and include cell phone tracking systems, video analysis software facial and iris recognition tools, wiretap operational tools, and a variety of intelligence gathering software tools able to hack suspect networks and or mimic cellphone towers to elicit signals from cell phones in a specific area (Federal Bureau of Investigation, 2008). These tools have not gone without controversy relating to encryption as well as illegal eavesdropping. The United States Secret Service has broad jurisdiction to investigate computer crime, including unauthorized access to protected computers, identity theft, distribution of denial of service (DDos) attacks involving disruption of electronic commerce or extortion, and distribution of malware (Federal Bureau of Investigation, 2008). The United States Secret Service (USSS) has established Electronic Crimes Task Forces (ECTFs) in approximately 39 cities across the country, bringing together the expertise of federal, state, and local agencies and representatives from industry and the academic community (United States

Secret Service, 1996). The mission of Electronic Crimes Task Forces (ECTF) is the prevention, detection, mitigation, and aggressive investigation of attacks on the United States, financial institutions and critical infrastructures. Many federal agencies participate in Electronic Crimes Task Forces (ECTF) and lead or serve other investigative task forces spread across the country. Among the federal agencies participating in these efforts are the United States Attorney's Office, the FBI, the United States Postal Inspection Service (USPIS), the U.S. Immigration and Customs Enforcement (ICE), the Social Security Administration (SSA) participation in approximately 100 such TFs. Many of these TF's are aimed at specific computer-assisted crimes, such as identity theft, advance fee schemes, and exploitation of children (United States Secret Service, 1996)..

The Comprehensive National Cybersecurity Initiative (CNCI) which was in the National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 (NSPS-54/HSPD-23) had three major goals: establishing a front-line defence against today's immediate threats; defending against the full spectrum of threat, and strengthening the future cyber security environment. In 2009, the White House released the Cyberspace Policy Review: Assuring a Trusted and Resilient Information Communications Infrastructure, which augmented the Comprehensive National Cybersecurity Initiative (CNCI) programs that were underway. It recommended near-term priorities including the clarification of roles, responsibilities, and agency authorities for cyber security across the federal government; the preparation of a cyber incident response plan; the initiation of a national public cyber awareness and education campaign; the establishment of a framework for research and development, and the appointment of a National Cyber Security Coordinator answering directly to the President. Since then, the US government has continued to release a number of supporting policies and documents outlining plans and intentions for cyber security. Congress has passed legislation targeted specifically at computer-related crimes. The government can charge computer crimes under at least forty different federal statutes and many traditional criminal statutes apply to computer crimes. Computer Fraud and Abuse Act of 1986 (CFAA) make it a felony to knowingly access a computer without authorization and with intent or reason to believe that the information obtained would be used to injure the United States or to benefit a foreign country. The federal Computer Fraud and Abuse Act (CFAA)

serve as the primary means by which unauthorized access to computer systems, including data access and theft cases, are prosecuted.

In 2009, Albert Gonzalez a former government informant was indicted on charges of conspiracy to gain authorized access to computers, to commit fraud in connection with computers and to damage computers, in the process stealing 170 million credits and debit card numbers (*United States v. Gonzalez,* 2009 U.S. Dist. LEXIS 50791). The case*, United States v. Rodriquez,* 628 F.3d 1258 (11th Cir.2010) is believed to be the largest hacking and identity theft case ever prosecuted in the United States (United States v. Rodriquez, 628 F.3d 1258 (11th Cir.2010). To combat unsolicited e-mails, United States Congress adopted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act). The CAN SPAM Act prohibits a number of well-known deceptive and or fraudulent practices commonly used in commercial e-mails. A federal appellate court, *in United States v. Kilbride*, 584 F.3d 1240 (9th Cir.2009), upheld the conviction for Jeffrey Kilbride who was sentenced to 78 months and Robert Schaffer who was sentenced to 63 months for violating the CAN-SPAM Act. United States Congress enacted the Undertaking, Spam, Spyware, and Fraud with Enforcers Beyond Borders Act of 2006 (SAFE WEB Act) to strengthen the ability of the Federal Trade Commission (FTC) to enforce the CAN-SPAM Act outside of U.S. borders. The Electronic Communication Privacy Act of 1996 (ECPA) also makes it illegal to intentionally intercept electronic transmissions and regulation of crimes with no close traditional crime analogue, such as hacking. This Act is in line with the Ghana Electronic Communication Act, 2008 (Act 775) which also makes it illegal to intentionally intercept the electronic transmission. The US Electronic Communication Act attempts to curb hacking activities by fortifying the privacy rights of computer users and enabling law enforcement officers to employ electronic surveillance in the course of investigating computer crimes. While federal officials often investigate and prosecute cybercrimes, state officials can also prosecute computer crimes under a variety of state laws.

6.6 RESEARCH QUESTION FIVE (5):

- **What are the successes and failures of the Ghana anti-cybercrime agencies in their fight against Virtual Crime and how can the legislative and regulatory framework in Ghana be improved to make them more effective and efficient in cybercrimes?**

6.6.1 THE ANTI-CYBERCRIME AGENCIES IN GHANA

The research established that Ghana has experienced a rapid expansion of access to the internet and current trends show no sign of slowing down. The research found that there are institutions or agencies such as cybercrime unit of Ghana police Service, Office of Special Prosecutor**,** Economic and Organised Crime Office, National Intelligence Bureau, are charged with the requisite legal mandate of investigating offenses relating to digital crime. It was emerged in the study that the there is also the Criminal and Other Offenses Act 30 of 1960 which mandates law enforcement agencies to search and seize evidence where necessary. The research has shown that there are robust legislative frameworks in place to deal with virtual crime or cybercrime offences, but specific provisions or sections are scattered in many legislations making it difficult to have a one uniform legislation for all virtual offences and prosecution. There are cyber security institutions and prosecutorial agencies set up by the Ghana government to deal with cybercrime-related offences and the prosecutorial process in a court of law. And they include:

6.6.2 THE ANTI-CYBERCRIME: INVESTIGATION AGENCIES IN GHANA

6.6.2.1 Cybercrime Unit of the Ghana Police Service

The Police Service is a single cohesive unit, organized on a national basis with a unified command under the leadership of the Inspector General of Police who subject to any directives from the Police Council is responsible for exercising general day-to-day supervision and control over the Administration and Operation of the Police Service. “The

Ghana Police Service has set up a specialized unit at the Criminal Investigations Department with its primary role as detection and investigations of crimes whereby digital device(s), network(s), another telecommunication device (s) or the internet space is/are the target(s), or the means used. The Cyber Crime Unit is equipped with a state-of-the-art Digital Forensics Laboratory for digital forensics examination and a Cyber Patrol Section for advanced online monitoring and surveillance of Ghana's cyberspace for crime detection. Cybercrime Unit to review and propose policies, laws, regulations, guidelines and standards on the management of fraud, corruption and cybercrime, to coordinate and provide guidance to all law enforcement agencies in fraud, corruption, cybercrime and other related offences, to Prepare charges, miscellaneous applications and other related documents, to Supervise corruption cases handled by other anti-corruption and fraud bodies, to Cooperate and liaise with government good governance entities and review relevant files from investigative organs, to Review relevant files from investigative organs.

The Cyber Crime Unit's involvement is not limited to criminal acts commonly associated with technology itself – such as hacking – but extends to investigations of more traditional offences such as fraud, threats, and other serious crimes whereas a digital device was the means used. The Cybercrime Unit also investigates sensitive cases such as online child exploitation and abuse and all other cases related to women and children on the internet space.

6.6.2.2 Economic and Organized Crime office

The Economic and Organised Crime Office (EOCO) was established by the Economic and Organised Crime Office Act 804 of (2010) as a specialised agency to monitor and investigate economic and organised crime and on the authority of the Attorney-General prosecute these offences to recover the proceeds of crime and provide for related matters. The institution is empowered to investigate, prevent and prosecute offenders who engage in money laundering, human trafficking, prohibited cyber activity, tax fraud,

foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and, other serious offences. Economic and Organised Crime Office (EOCO) is responsible for identifying, tracing, freezing, confiscating, or seizing proceeds or recovering the proceeds of crime, monitoring activities connected with the offences taking reasonable measures necessary to prevent the commission of crimes and their correlative offences, disseminating information gathered in the course of investigation to law enforcement agencies, other appropriate public agencies and other persons the Office considers appropriate in connection with the offences co-operate with relevant foreign or international agencies in furtherance of this Act and perform any other functions connected with the objects of the Office.

6.6.2.3 The National Intelligence Bureau (NIB)

The National Intelligence Bureau (NIB) is the internal security intelligence agency of Ghana. The NIB has been empowered through Security and Intelligence Agencies Act 1030 of 2020 to arrest or detain and interrogate over a wide arrange of criminal offenses that includes organised crime, financial crime, espionage, terrorism, drug trafficking, cybercrime and provide intelligence to counter threat to Ghana nation security and by the President or the council. The Bureau is an integral part of the National Security Council which combats matters of counter intelligence and homeland security. The BNI has undisclosed offices in all the sixteen regions of Ghana.

6.6.2.4 The office of Special Prosecutor (OSP)

In 2018 the government of Ghana established the Office of Special Prosecutor as a specialized independent anti-corruption agency in Ghana, in pursuance of the United Nations Convention against Corruption. The Office of Special Prosecutor is enshrined with powers mainly from the Office of the Special Prosecutor Act, 959 of (2017), Office of the Special Prosecutor Regulations L.I. 2373 (2018), Office of the Special

Prosecutor (Operations) Regulations L.I. 2374 (2018), and other laws bearing on the suppression and repression of corruption.

The Special Prosecutor, the Deputy Special Prosecutor and officers of the Office of the Special Prosecutor have the powers of a police officer under the criminal and other Offences (Procedure) Act, 1960 (Act 30) and under any other law. The powers of the OSP include: Arrest Search and take possession of documents, Seizure of suspected tainted property – movable and immovable, Seizure and detention of currency suspected to be proceeds of corruption, Direct declaration of property and income, Freezing of property, Render orders for disclosure of funds and other assets, Render confiscation orders, Protect witnesses, victims, whistleblowers and informants. The OSP has the object of investigating and prosecuting specific cases of alleged or suspected corruption and corruption-related offences in the public and private sectors, recovering the proceeds of such acts by disgorging illicit and unexplained wealth and taking steps to prevent corruption. The specialized attribute of the OSP particularly lies in its fortification with the cure of the inadequacies of the existing anti-corruption agencies by being designed as a comprehensive anti-graft agency with investigative, prosecutorial, intelligence gathering, surveillance, and counter-surveillance, police, national security, and revenue-generating powers. In addition to taking its initiative, the OSP also receives and acts on referrals of investigations of alleged corruption and corruption-related offences from Parliament, the Auditor-General, the Commission on Human Rights and Administrative Justice, the Economic and Organised Crime Office, and any other public institution. The Office also receives and acts on complaints from private entities and individuals

6.6.3 THE ANTI-CYBERCRIME: PROSECUTORIAL AGENCY IN GHANA

6.6.3.1 The Attorney General Department

In Ghana, the powers to prosecute cybercrime offence are vested in the Attorney General. The Attorney General Department is an office established under the 1992 constitution of Ghana. The Attorney General (AG) prosecutes all crime offenders on behalf of the

Republic. The Ministry of Justice and Attorney General's Department has been charged with the responsibility of prosecuting offenders. All investigations by the anti-cybercrime agencies such as cybercrime unit of Ghana police Service, Office of Special Prosecutor**,** Economic and Organised Crime Office, National Intelligence Bureau (NIB), ends up with the Attorney General who offers legal advice on the next step to take.

6.6.4 THE ANTI-CYBERCRIME: CYBERSECURITY AGENCIES AND POLICIES IN GHANA.

6.6.4.1 Cyber Security Authority

The Ghana Government has established the Cyber Security Authority through the Cybersecurity Act 2020 (138) to control and supervise cybersecurity activities in the country and rise to a higher standard of the development of cybersecurity activities in the country thereby providing for related matters concern. This Agency started as the National Cybersecurity Secretariat (NCSS) with the appointment of an advisor for National Cybersecurity in 2017 but in 2018 it was the transition to the National Cybersecurity Centre (NCSC) as an agency under the Ministry of Communication (Now Ministry of Communication and Digitalization) until it started full operation as Cyber Security Authority (CSA) in October 2021 (Cyber Security Authority, 2021). As the government under the Ministry of Communication and Digitalization, the Cyber Security Authority has the responsibility to regulate the activities of cybersecurity in the country and prevent, manage, and respond to threats and incidents of cybersecurity infrastructure. Regulation of owners of Critical Information Infrastructures in respect of cybersecurity activities, cybersecurity service providers and practitioners in the country are under the supervisor of the authority. The authority promotes the development of cybersecurity in the country to ensure a secured and resilient digital ecosystem, collaborates with international agencies to promote the cybersecurity of the country and creates or establishes a platform for cross-sector engagements, on matters of cybersecurity for effective coordination and cooperation between key public institutions and the private sector.

6.6.4.2 Computer Emergency Response Team (CERT)

In 2014 the government of Ghana set up a national Computer Emergency Response Team (CERT) to address all cyber security related crimes and problems and will also work to halt internet fraud (Sakawa) and stop the abuse of children online in Ghana. Computer Emergency Response Team Ghana (CERT-GH) coordinates security incidents on behalf of its constituency and has no authority to reach further than that. CERT-GH is however expected to make operational recommendations regarding vulnerabilities and mitigation of incidents and/or incident handling. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such recommendations is not the responsibility of CERT-GH, but solely of those to whom such recommendations are made (Computer Emergency Response Team, 2014). CERT-GH is authorised to address all types of computer security incidents which occur, or threaten to occur, in our Ghana and which require cross-organisational coordination." The level of support given by CERT-GH will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and CERT-GH's resources at the time. Special attention will be given to issues affecting critical infrastructure (Computer Emergency Response Team, 2014).

6.6.4.3 National Information Technology Agency (NITA)

The National Information Technology Agency is a public service institution established by Act 771 in 2008 as the ICT policy-implementing arm of the Ministry of Communications (National Information Technology Agency , 2008). "NITA is the agency responsible for implementing Ghana's IT policies. Its mandate includes identifying, promoting and developing innovative technologies, standards, guidelines and practices among government agencies and local governments, as well as ensuring the sustainable growth of ICT via research with development planning and technology acquisition strategies to facilitate Ghana's prospect of becoming a technology-driven, knowledge-and values-based economy as espoused in the e-Ghana project which ideally seeks to assist the Government to generate growth and employment, by leveraging ICT and public-private

partnerships. The agency is further empowered to give accreditation to individuals who want to conduct legitimate business online (Ennin and Mensah 2019:38). The establishment of the National Information Technology Agency is essential for the e-Government to take off in Ghana. E-Government, being an essential component of the e-Ghana project will contribute to improved efficiency, transparency and accountability in selected Government functions." Under this Act, the functions and responsibilities of the agency are captured in clause 3 which stipulates that the Agency shall(National Information Technology Agency , 2008):

(a) Perform the functions of the certifying Agency established under the ETA, 2008 (Act 772).
(b) Issue licenses and ensure fair competition among license holders in cyberspace.
(c) Monitor, enforce and ensure effective compliance with the conditions contained in licenses and tariffs.

6.6.4.4 Ghana National Cyber Security Policies and Strategy (NCSP)

The National Cyber Security Policy (NCSP) seeks to address the risks to the Critical National Information Infrastructure (CNII) which comprises the networked information systems of ten critical sectors. The policy recognises the critical and highly interdependent nature of the CNII and aims to develop and establish a comprehensive program and a series of frameworks that will ensure the effectiveness of cyber security controls over vital assets. It is being developed to ensure that the CNII is protected to a level that comensurate the risks faced. The policy has been designed to facilitate Ghana's move towards a knowledge-based economy and will be based on several frameworks that comprise legislation and regulations, technology, public-private cooperation, and institutional and international aspects. The expansion of Internet access in Africa, representing the largest growth in the world, means more people today have access to the Internet, with its attendant risks of attack from people with disruptive tendencies to defraud other Internet users and commit cybercrimes. These disruptive activities by cyber criminals have caused the debate on cyber security to be on the top of the agenda for almost every country, and many countries are strategizing on how to combat

cybercriminals. Several global initiatives are also addressing cybercrime and the enhancement of cyber security. The cyber menace in Ghana has been more of cyber fraud. The popular "sakawa" where cybercriminals defraud unsuspecting Internet users of large sums of money in Ghana and abroad remains prevalent because of inadequate laws on cybercrime to prosecute cyber criminals.

The Electronic Transaction Act (2008) has provisions for law enforcement agencies to fight cybercrime. However, this is not adequate for law enforcement in the fight against cybercrime as there are legal gaps caused by rapid change in the cyber landscape. There is, however, the need to fully address all aspects of cyber security, and apply a multi-stakeholder approach to fighting the cyber menace. Several initiatives are ongoing to address the cyber menace, all of which need to be brought under one umbrella for Ghana. In recent times, Ghana has experienced a several cyber-attacks including the defacing of a number of government websites by Internet hackers. These attacks have a denting effect on the cyber image of Ghana and are indications of security weakness of our cyber infrastructure and space. Cyber-attacks have become very sophisticated and widespread and many countries are not only focusing on protecting their critical information infrastructure but also ensuring that there are very good incident response teams in place to respond to incidents cyber security incidents.

6.6.4.5 Information Communication and Technology for Accelerated Development

In June 2003 Ghana Government introduced and signed a policy document on Information and Communication Technology (ICT) for Accelerated Development. “Nations worldwide have recognised the developmental opportunities and the challenges of the emerging information age characterized by ICT. These technologies are driving national development efforts worldwide and a number of countries in both the developed and developing world are exploring ways of facilitating their development process through the development, deployment and exploitation of ICT within their economies and societies. The Ghana ICT for Accelerated Development (ICT4AD) Policy represents the

Vision for Ghana in the information age. The development of this policy framework was based on a nationwide consultative process involving all key stakeholders in the public sector, private sector and civil society. In line to pursue a multi-sectorial development policy targeting key sectors of the economy as stated in a number of Ghana's socio-economic development policy frameworks including the Vision 2020, the Ghana Poverty Reduction Strategy Paper and the Co-ordinated Programme for Economic and Social Development of Ghana (2003-2012). The Government is committed to, the establishment of a globally competitive, diversified and balanced economy that is driven by information, knowledge and skills --- an economy with an ICT-intensive modern industrial sector; a modern, efficient and competitive agricultural sector; and a vibrant ICT driven, valued added service sector capable of serving as the engine for accelerated economic growth and development.

Among the objectives of the policy (Ghana ICT for Accelerated Development, 2003) are:

(a) To create the necessary enabling environment to facilitate the deployment, utilization and
(b) the exploitation of ICT within the economy and society
(c) To support the development of a viable knowledge-based ICT industry to facilitate the production, manufacturing, development, delivery, and distribution of ICT products and services
(d) To facilitate the modernization of the agricultural sector through the deployment and exploitation of ICT to improve its efficiency and productivity.
(e) To support the development of a competitive high value-added services sector, to serve as an engine for accelerated development and economic growth with the potential to develop into a regional business-services and ICT hub.
(f) To aid the process of the development of national human resource capacity and the nation’s Research and Development capabilities to meet the changing needs and demands of the economy
(g) To promote an improved educational system within which ICT are widely deployed to facilitate the delivery of educational services at all levels of the educational system
(h) To facilitate a widespread deployment and exploitation of ICT within society to support the delivery of health and social services
(i) To support the modernization of the civil and public service through institutional reforms, renewal and the deployment and exploitation of ICT to

facilitate improvements in operational effectiveness, efficiency and service delivery

(j) To facilitate the development, expansion, rehabilitation and continuous modernization of the national information and communications infrastructure

(k) To guide the development and implementation of electronic government and governance, as well as electronic commerce and business strategies and action plans

6.7 EXTEND VERSION OF THE RESEARCH PROBLEM

Chapter 1: contextualised the study by outlining the research problem, research questions, research objectives and limitations, and research design and methodology and provides an overview of the entire study. Furthermore, clarification of specific and important terms and concepts in cybercrime investigations and electronic evidence was captured. Preliminary findings in Chapter 1 were that cybercrime is a serious problem in Ghana. This has been confirmed by both the Cybercrime Unit of the Ghana Police Service in 2019 and the computer Emergency Response Team under the Cyber Security Authority in Ghana. As of September 2021, the Cybercrime Unit of the Criminal Investigations Department (CID) of the Ghana Police Service said cyber frauds represented 45% of all cybercrime cases, making it the topmost. Cyber frauds were also ranked second in terms of the amounts of money stolen by cybercriminals. The statement corroborated the financial loss the country incurred over the past years. According to the Computer Emergency Response Team Ghana lost $105 million in 2019 and $9.8 million12 in 2018 due to internet fraud and cybercrime (Eric Appah Marfo September 3, 2021). For instance, 2019 showed no improvement in Ghana's cybercrime cases from 2018. Like in 2018, Ghana has still ranked as a top most destination for cybercrimes and related cases. Ghana's ranking in cybercrime, according to the Interpol report (2020 – Africa cyber threat assessment), is a figuratively long distance from the countries that the study used for comparative purposes. Whereas Ghana's government is striving for measures to combat cybercrime and its related methods for investigation, the United States, United Kingdom, Australia and South Africa have put in place measures and instituted agencies to reduce the menace and prosecute culprits.

In Chapter 2, A Thematic Reflection on Extant Literature on digital crimes, Internet vulnerabilities and classification of digital criminal activities against persons, property, government, and society. The motives and causes of cybercrime perpetrators were also discussed in this chapter. In particular, the chapter addressed virtual crimes against the government in which certain offences are committed or done by a group of persons intending to threaten the international governments by using internet facilities which include cyber terrorism. Cyberterrorism is a major burning issue in domestic as well as a global concern. The common form of these terrorist attacks on the Internet is by a distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyberterrorism activities endanger the sovereignty and integrity of the nation**.**

Chapter three of the research explored computer forensics, its sub-disciplines and the detective work done by law enforcement and other investigators. The chapter provided Legal issues and investigative procedures of virtual criminal investigation approaches and challenges. Significant points of convergence have been noted on the cybercrime unit of the Ghana police, South Africa's electronic crime unit, Australia's high tech crime center, US department of justice cybercrime section, UK's national cybercrime unit and comparative analysis were explored to see the uniqueness of investigations methods and other alternative methods of processing digital crime scene for evidence gathering. This chapter emphasised that when conducting a crime scenes investigation, the investigator first needs to establish the legal authority to perform a search. Once at the crime scene, the boundaries of the scene need to be established and investigators should carry all the forensic toolkit that contains gloves, pens, labels, tags, evidence bags, plastic ties, coloured tape, and other items necessary for this purpose. This chapter pointed out that an investigator should photograph, document, and label all the ports and cable connections and place evidence tapes over ports, power switches, and disk drives.

Chapter four provided a micro comparison approach to criminal procedures rules and related issues of electronic evidence search with and without a warrant. The chapter addressed. The chapter focused on the main problems in ensuring the integrity of digital evidence in digital forensic investigations, and addressed the fundamental principles

related to the correct procedures to be followed during digital search and seizer and point out some of the legal concepts of digital evidence search with or without a warrant and other search warrant exceptions. Various search methods for digital evidence were explored.

Chapter five explored on virtual evidence perspectives in terms of admissibility and evidential weight. Today's criminals are using computers as their tools to take advantage of new technological possibilities. The digital forensic investigator or law enforcement has to be prepared to investigate criminal acts and authentication of virtual evidence in criminal and civil proceedings, rules of admissibility for evidence, weight, credibility and sufficiency of virtual evidence. The chapter also explored the role of judges in evaluating and admitting virtual evidence. Legal issues on the admissibility of virtual evidence in Ghana, United States of America (USA), Australia, United Kingdom (UK) and South Africa were compared.

Chapter six of this research outlined and addressed all the research questions in the study. The first question (question 1) in this study was addressed to understand the prevailing legal issues and challenges of virtual criminal investigations in the current laws governing cybercrime. The chapter addressed the research question two (2) of the study which focused on the main problems in ensuring the integrity of digital evidence in digital forensic investigations, and addressed the fundamental principles related to the correct procedures to be followed during digital search and point out some of the legal concepts of digital evidence search with or without a warrant and other search warrant exceptions. Various search methods for digital evidence were explored. The Chapter addressed the research question three (3) of the study which focused on the cybercrime legislation principles and its applications towards digital forensic investigation and admissibility of virtual evidence for prosecution. The Chapter also addressed the research question raised in question four (4) of the study which focused on the key national legislative framework in Ghana's regional boundaries and international framework and obligations to combat Virtual criminal activities or Cybercrime. The Cybersecurity institutions such as the Financial Forensic and Cybercrime Unit of Ghana Police, Computer emergence and

response team (CERT), Office of the Special Prosecutor, National Information Technology Agency, and Economic and Organized Crime Office were explored. It was concluded that the limitation of the common law and its narrowness when dealing with cybercrime calls for the enactment of the Electronic Transactions Act and other laws which attempted to address the issues of cybercrime. Cybersecurity will continue to remain a growing important issue and Ghana as a country should see it as a matter of concern for national security. Although there are legislations and policy frameworks for cybersecurity institutions to fight against the menace but there remains a lack of engagement on an international level. This chapter also points out and addressed question five (5) of the study which focused on the successes and failures of the Ghana anti-cybercrime agencies in their fight against virtual crime or digital crime. In terms of the findings, a number of best practices in these jurisdictions are noted and possible lessons for Ghana are identifiable. It was revealed that the United States of America, United Kingdom, Australia and South Africa have some efficient anti-cybercrime agencies in their fight against cybercrime.

6.8 SUBMISSIONS AND RECOMMENDATIONS

The submissions and recommendations in this section are postulated in thematic forms to properly depict and capture the problems identified in this study.

6.8.1 Establishment of Independent Anti-Cybercrime Units in regions of Ghana

It is recommended that Ghana must establish an independent cybercrime directorate in all the regions of the country which will be dedicated to systematically dealing with the cybercrime menace. The implementation of these strategies was to form an effective structure for increasing Ghana's cyber security by enhancing the sharing of information to provide a targeted, de-conflicted, national response. This strategy provided the foundation for the creation of a new National Cyber Security Centre (NCSC) under the ministry of communication which is pivotal to improving communications and de-

confliction among relevant organisations. The establishment of a regional cybercrime unit will enhance law enforcement in its fight against cybercrime at the regional level.

6.8.2 Enactment of uniform Legislation on Digital or Electronic Evidence

Aside from the Constitution, some laws are in existence to provide law enforcement agencies powers to investigate crime and gather evidence and present the evidence in a way that is admissible in court. One such law for the arrest and detention of suspected offenders is the Criminal Offenses Act (Criminal Code) 1960, known as Act 29 (Act 29, 1960). The Evidence Act 1975 is another important legislation for the investigation and prosecution of offences. Sections 51 and 52 of the Evidence Act 1975 give the court discretion to accept evidence in prosecution. Even though there is a plethora of legislation on investigations and prosecution of crime and related cyber offences, these legislations are scattered in various acts and laws making it strenuous for law enforcement agencies to apply during digital evidence search, collection, and handling. Harmonising the existing legislation into a uniform one with broad comprehensiveness will enhance law enforcement and judges in their prosecution of cybercrime. The Attorney General of Ghana should set up a Cyber or digital Law Review Committee to bring all Digital or Cyber Law Luminaries and Cyber forensic experts and other stakeholders together in order to identify the challenges in the cyber landscape and propose a comprehensive legal framework that deals specifically on cyber-related crime and prosecution.

6.8.3 Establishment of an Independent Anti-Cybercrime Court

Cybercrime is so prevalent among the youth and even some learned intellectuals in Ghana. “In 2019 and 2018 respectively Ghana lost a total of $114.8 million to cybercrime. The years witnessed some of the most sophisticated online crimes and new forms of malware that target both human and technical weaknesses in a business, accompanied by huge losses. Therefore, a specialised independent anti-Cybercrime court (IACC) must be established with dedicated resources to deal with cybercrime and electronic-related cases, particularly this court will work with the Cybercrime unit of the Ghana Police, Economic and Organised Crime Office, and the Office of Special Prosecutor."

6.8.4 Strengthen Sanctions for Cybercrime

It is recommended that policy formulation on specific-minimum sentencing guidelines for cybercrime or minimum sentencing legislation for electronic-related cases and offences be modelled on the electronic transactions Act and Criminal Code Act. Alternatively, these Acts must be amended and inserted into it a substantive provision for the sentencing of cybercrime offenders. This recommendation takes into account the discussions in Chapter one (1) with regard to losses in cybercrime. Particularly, consider the approach of the sentencing guidelines for Cybercrime in the United States, United Kingdom, Australia and South Africa. There should be a rejection of the small sentencing imposed for cybercrime offenders in Ghana.

6.8.5 Establishment of National guidelines for Digital Evidence Collections

The national agencies that are responsible for cybercrime investigations and related digital evidence collections should be redeveloped and guided by principle. “The Association of Chief Police Officers (ACPO) of the United Kingdom and Department of Justice of the National Security has set guidelines for cybercrime investigations and electronic evidence. The Department of Justice and Association of Chief Police Officer guidelines could be adopted by Ghana to enhance the legal fraternity as a guideline on cybercrime investigation and digital evidence collection for law enforcement in the public sector and private investigators. There should be an enhancement in the capacities of law enforcement investigators to strengthen digital forensic investigations and prosecutions. The regulation, accreditation and certification of forensic services is a major concern in Ghana and therefore this capacity building on the appropriate guidelines will improve law enforcement and investigators' responsibilities of overseeing all issues of cybercrime and digital forensic investigation and regulations to avoid a miscarriage of justice as results of low-quality forensic services. Evidence is not the only thing that is subject to tests of admissibility.

A forensic examiner’s qualifications can be challenged or the tools or methodologies used in a forensic investigation can be objected to. From 1923 to 1993, the test for admissibility of expert witness testimony and methodologies was based on the 1923 ruling in *Frye v*

United States (1923) The Frye test as it came to be known, requires that the scientific principle upon which the work is based s sufficiently established to have gained general acceptance in the particular field in which it belongs. Using *Frye,* a judge had to test the admissibility of expert testimony before allowing it in court. In part because of the problems caused by the general acceptance criteria the Frye test that Federal Rule of Evidence 702 had been relying on was replaced or superseded by the Daubert test in 1993. In 1993, the Supreme Court of the United States issued an opinion in the case of *Daubert v. Merrell Dow Pharmaceuticals* 509 U.S. 579 (1993) that abandoned the earlier Frye standard in federal cases and set a new standard. Therefore, judges in Ghana must take into account the following":

(a) Whether the theory or technique can be and has been tested
(b) Whether it has been subjected to peer review and publication
(c) The known or potential error
(d) The general acceptance of the theory in the scientific community
(e) Whether the proffered testimony is based upon the expert's special skills

The Daubert test is primarily a question of relevance or "fit" of the evidence. It recommended that courts hold that in order for testimony to be used it must be sufficiently tied to the facts of the case to help understand an issue being disputed (Norberg, 2006:112).

6.8.6 Develop Registered Anti-Cybercrime Tool-Kit for the Collection of Digital Evidence.

The widespread use of handheld smartphones and other devices capable of recording audio and video means that user generated recordings (UGRs) are increasingly presented as evidence in criminal investigations. An investigator or law enforcement for audio forensic needs to determine whether the integrity of the recording could be compromised, either deliberately or inadvertently, during the process of investigation. Creation of Registered Anti-Cybercrime Toolkit can assist the proposed Ghana Regional

Cybercrime Units by providing guidance on integrity and authentication of digital forensic evidence. The Anti-Cybercrime Tool-Kit should specify the first responder registered took-kit that will be used by law enforcement and investigators for cybercrime cases prior to any potential evidence collection. Comparatively, the USA has created a registered toolkit for all cybercrime investigation and electronic evidence collections for all its Federal Investigative Bureau Personnel. The national registered first responder toolkit is a set of tested tools designed to help in collecting genuine presentable evidence and understand the limitations and capabilities of electronic evidence at the time of collection. Creating a national registered tool-kit will makes the Anti-Cybercrimes investigators familiar with computer forensic tools and their functionalities and it will bolstered further research on digital forensic equipment's and technology.

6.8.7 Develop the National Anti-Cybercrime Investigation Strategy.

The Council of Europe Convention on cybercrime, to which Ghana has ascended to be a party, requires State Parties to develop and implement a comprehensive National Anti-Cybercrime investigation Strategy. "To respond to this obligation, this proposal could take lead in establishing the anti-cybercrime investigation strategy and action plan. Comparatively, for example, in 2018 the United State White house provides a National Cybersecurity Strategy to Protect America's national security and promote the prosperity of the American people. Furthermore, Comparatively, for example, in 2022 the Australia Government has come out with a national plan to combat cybercrime. If this recommendation is taken, such a comprehensive document should be developed to manage cybersecurity risks to increase the security and resilience of the Ghana Nation's information and cyber infrastructure systems that lists expected outcomes as the effective management of cybersecurity vulnerabilities." The strategy document must contain a framework with goals and strategic objectives with realistic implementation timelines.

6.8.8 Develop powerful technical Infrastructure for National Anti-Cybercrime Units

Today's battles between corporations, governments, and countries are no longer fought only in the typical arenas of boardrooms or battlefields using physical force. Now the battlefield starts in the technical realm, which ties into most of modern-day life. Therefore,

It is recommended that the government build the necessary requisite cyber security infrastructure to safeguard Ghana's cyberspace. Because of this, the Government through the Ministry of Communication should increase resource allocations to the country's Anti-Cybersecurity agencies to set up the needed infrastructure to mitigate the increasing cyber threats. Also, since cybercrime perpetrated on the internet is borderless. The capacity building should include infrastructure that can enhance jurisdictional collaboration for cybercrime investigations and prosecution. It is submitted Ghana must develop a monitoring and evaluation plan as a matter of urgency to operate as a framework or strategic document to combat cybercrime and improve digital evidence collections.

6.9 FUTURE RESEARCH

This thesis summarises the cybercrime investigation and the position of legal issues and challenges to date on the searches with or without a warrant on digital evidence, authentication of evidence and the role of admissibility of digital evidence in the courtroom. It is submitted that while the Electronic Transactions Act 772 of 2008, and other related Acts in Ghana may be adequate to admit electronic evidence, some future research are required in order to properly recognise that cybercrime investigations and admissibility of digital evidence is fundamentally different to traditional crime and admissibility of physical evidence in the courtroom. Following discussions and findings in this study, the following areas or issues for further research have been identified:

(a) Conduct further research or study to investigate why the existing legislation is failing to combat cybercrime and related digital forensic investigations and to consider how to strengthen anti-Cybercrime institutions and the associated legislative frameworks.
(b) Investigate the obstacles to implementing a mandatory cybersecurity framework for government-owned critical infrastructure.
(c) Investigate how the ever-changing new cyber infrastructural devices market affects the work of forensic investigators

(d) Conduct research or study on how important is the testimony of a computer forensic witness to cases in the courtroom.

6.10 CHAPTER SUMMARY

A move forward into the cyber landscape or the information age has been increasingly clear for every nation and there must be a comprehensive legal framework to combat cybercrime. A lawbreaker or criminal armed with a computer and an internet connection has the capability to victimise people and access private information and computer systems illegal anywhere in the world. This research came about because of the necessity to enhance the general knowledge of cybercrime investigation and legal issues and challenges in collecting, handling analyzing, preserving and presenting electronic evidence at trial or in courtroom for prosecution. This research focused on the investigation of cybercrime and the collection of /digital evidence with or without a warrant by the investigator or law enforcement without compromising or tampering with its integrity or credibility. The study also focused on the guidelines and standards or requirements for admitting electronic evidence at the trial in the courtroom. The process of investigation requires the investigator to collect and preserve electronic evidence in a manner that can withstand any legal scrutiny at trial. Investigators need to be properly trained and skilled in handling electronic evidence. Human ingenuity has provided us with a great gift, cyberspace. This blooming network of computing communication technologies is quickly changing the Ghanaian community and our behaviour in it. Already the most common way a computer is involved in criminal activity is as a container of evidence. It turns out that few laws limit what can be done with cyber-criminal activities and one size–fit all legislation default rule is “inefficient” for eradication of cybercrime. By contrast, the flip cost of cyber-criminal activities and tampering of digital evidence for the prosecution of digital criminals are huge and therefore it is necessary to put out the right

skills, technical infrastructure, comprehensive legal framework, policies and strategies to combat the cybercrime canker.

The Electronic Communication Act 775 of 2008, National Information Technology Agency Act 771 of 2008, Data Protection Act 843 of 2012**,** Electronic Transaction Act 772 of 2008, and Ghana's Cybersecurity Act 1038 of 2020, enacted by the government of Ghana are all in the right direction to deal with cybercrime in Ghana but there is room for improvement on the digital investigation methodology and procedures. Because of the borderless nature of the internet and the challenges that it poses in terms of jurisdictional issues and lack of uniform legal cooperation, the government of Ghana must learn from other countries efforts to deal with cybercrime and its investigations and prosecutorial procedures. Ghana can learn from the approach used by the United States and other advanced countries which have well-established initiatives and methodologies in digital forensic investigation to develop and enhance their laws relating to electronic evidence and digital forensic investigation, and how to predict computer-related threats. Additionally, the Electronic Communication Act 775 of 2008, National Information Technology Agency Act 771 of 2008, Data Protection Act 843 of 2012**,** Electronic Transaction Act 772 of 2008, and Ghana's Cybersecurity Act 1038 of 2020 are relevant legal instruments that enhance and influence numerous legal transactions online. Upon all the concerns raised on these legal instruments, it can be seen and regarded as a step in the right direction in securing electronic commerce activities which can contribute towards the economic growth of Ghana.

REFERENCES

Adams, 2016. "Anticipatory Search Warrants: Constitutionality, Requirements, and Scope," *Kentucky Law Journal*: Vol. 79: Iss. 4, Article 4.

Adler, E.M. with Clark, R. 2011. An invitation to social research: How it's done.

Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C., 2011. Systematic Digital Forensic Investigation Model. International Journal of Computer Science and Security (IJCSS), 5(1), pp. 118–131.

Ajayi E.F.G 2015. Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, Vol.6(1), pp1-12.

Alkaabi, Mohay,Mccullayh and Chantler 2010. Dealing with the Problem of Cybercrime. information Security Institute, Queensland University of Technology, GPO Box 2434, 126 Margaret Street, Brisbane, QLD 4001, Australia.

Ameer Pichan, Mihai Lazarescu, and Sie Teng Soh. Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis. Digital investigation, 13:38–57, 2015.

Amna Eleyan, Derar Eleyan, (2015) "Forensics Process as a Service (FPaaS) for cloud computing", European Intelligence and Security Information Confernece.

Ana I. Cerezo, Javier Lopez and Ahmed Patel, 2007 International Cooperation to Fight Transnational Cybercrime: Conference Paper. https://www.researchgate.net/publication/427382

Anderson, V. 2014. Research methods in human resource management: Investigating a business issue. 3rd edition. London: CIPD house.

André Å., 2018 Digital Forensic. 1ST edition. John Wiley and Sons Ltd. West Sussex.

Ariel B, Sutherland A, Henstock D, et al. 2016a. Wearing body cameras increases assaults against officers and does not reduce police use of force: Results from a global multi-site experiment. European Journal of Criminology 13(6).

Asghar, J. 2013. Critical Paradigm: A Preamble for Novice Researchers. Life Science Journal, 10(4): 3121.

Association of Chief Police Officers (2012)

Astalin, P.K. 2013. Qualitative research designs: A conceptual framework. International Journal of social sciences and interdisciplinary research. 2(1):118-124.

Australian High Tech Crime Centre, (2008)

Australian High Tech Crime Centre, (2013)

B. Fisher and D.R. Fisher 2012. Techniques of Crime Scene Investigation (Forensic and Police Science) 8th Edition, Taylor and Francis Group LLC Baton Raton, Florida.

Babbie, E. with Mouton, J. 2012. The practice of social research. South African edition. South Africa: Oxford university press.

Badenhorst, C. 2014. Research writing: Breaking the barriers. Pretoria: Van Schaik

Barbara California

Baryamureeba, V. and Tushabe, F., 2004. The Enhanced Digital Investigation Process Model. In Proceedings of the Fourth Digital Forensic Research Workshop. pp. 1–9.

Basdeo, V.M., Montesh, M. and Lekubu 2014. B.K. 2014. search for and seizure of evidence in ... Journal of Law, Society and Development. (V1) 48–67.Basics of Social research: qualitative and quantitative approaches.

Berg, B.L. with Lune, H. 2012. Qualitative research methods for the social sciences. 8th edition. USA: Pearson.

Bergman Paul and Sara J. Berman Barrett. Represent yourself in Court: how to prepare and try a winning case, 5th edition. Berkeley CA

Bless, C., Highson-Smith, C. with Sithole, S. 2013. Fundamentals of social research methods: an African perspective. 5 th edition. Cape Town: Juta Company Ltd.

Bless, C., Higson-Smith, C. with Sithole, S. L. 2014. Fundamentals of social research methods: An African perspective. 5th edition. Cape Town: Juta.

Braun, V. and Clarke, V. 2013. Successful Qualitative Research: A Practical Guide for Beginners. SAGE Publication, London.

Brenner 2011 Cybercrime: Criminal Threats from Cyberspace, School of Law Faculty Publications, University of Dayton.

Brenner and Koops 2004 "Approaches to jurisdiction" 2004 (4) Journal of High Technology Law 1-46

Brenner, Bert-jaap and Koops 2004 "Approaches to jurisdiction" 2004 (4) Journal of High Technology Law 1-46

Brooks, J. D. 2004. Valid Searches and Seizures without Warrants. A

Bruce, C. 2014 Identifying, Weighing, and Prioritizing Repeat Offenders (Video webinar)

Bryman, A 2012. Social Research Methods. 4th edn. Oxford: Oxford University Press

Bryman, A. and Bell, E. (2015) Business Research Methods. Oxford University Press, Oxford.

Cahyani, N. D. W., Ab Rahman, N. H., Glisson, W. B., & Choo, K.-K. R. 2017. The role of mobile forensics in terrorism investigations involving the use of cloud storage service and communication apps. Mobile Networks and Applications, 22(2), 240

Cameron S. D. Brown 2015. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barries to Justice. International Journal of Cyber Criminology Vol.9, Issue 1

Carrier, B. and Spafford, E.H., 2003. Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2(2), pp. 1–20.

Carrier, B. and Spafford, E.H., 2004. An Event-Based Digital Forensic Investigation Framework. In Digital Forensic Research Workshop. pp. 11–13

Casey E. 2011. Digital Evidence and Computer Crime: Forensic Science, computers. Elsevier

Cassim, F. (2009). Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study.

Chang, Zhong & Grabosky (2018); citizens co-production of cyber security:Self-help, vigilantes and cybercrime. Regulation and Governance Wiley

Choo and Dehghantanha (2016) Contemporary Digital Forensic Investigations of Cloud and Mobile Applications Elsevier Inc.

Cohen, F.B. (1991). A Formal Definition of Computer Worms and Some Related Results. Pittsburgh, PA 15217, USA.

Cohen, L., Manion, L & Morrison, K. 2017. Research methods in Education. 8th edition. Oxon, Routledge.

Cole, B. (2013). Cybercrime is real and it’s here. iol News.

Commonwealth Parliament (2019)

Cooper, D.R with Schindler, P.S. 2014. Business research methods. 12th edition. Boston: McGraw- Hill International edition.

Cooper, D.R. with Schindler, P.S. 2011. Business research methods. 11th edition. Boston: McGraw-Hill International edition.

Council of Europe Convention on Cybercrime (2013)

Creswell, J, W. (2013). Qualitative inquiry and research design: Choosing among five Approaches. (3thEd). Los Angeles: Sage Publications

Creswell, J. W. with Plano Clark, V, L. (2011). Designing and conducting mixed methods research. 2nd ed. Thousand Oaks, California: Sage Publications.

Creswell, J.W. (2009). Research design. Qualitative, quantitative and mixed methods approaches. (3thEd).

Creswell, J.W. 2014. Research design: International student edition. 4th edition. Washington DC: Sage.

Creswell, J.W. 2015. Research design: qualitative, quantitative and mixed methods approaches.3rd edition. USA: Sage.

Cross C (2018). Denying victim status to online fraud victims: The challenges of being a 'nonideal victim'. In M Duggan (ed), Revisiting the ideal victim concept: Developments in critical victimology. Bristol, UK: Policy Press: 243–62

Cross C (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. International Journal of Law, Crime and Justice.

Cross C (2018). Victims' motivations for reporting to the 'fraud justice network.' Police Practice and Research 19(6): 550–564

Cross C, Richards K & Smith RG (2016). The reporting experiences and support needs of victims of online fraud. Trends & issues in crime and criminal justice no. 518. Canberra: Australian Institute of Criminology.

Cybersecurity ventures 2021. cybersecurityventures.com / top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021

Daniel Ennin, Ronald Osei Mensah 2019. Cybercrime in Ghana and the Reaction of the Law Journal of law, policy and globalization.

De Vos, et al 2011. Research at grass roots: For the social sciences and human service professions. 4th edition. Pretoria: Van Schaik.

De Vos, et al 2011. The sciences and the professions. Pretoria: JL Van Schaik Publishers.

Deng and Mason (2016). Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012)

Denscombe, M. 2010. The good research guide for small-scale social research projects. 4th edition. England: McGraw-Hill.

Denscombe, M. 2015. The good research guide: For small scale social research projects. 6th edition. England: Open University press.

E. M. Robinson (2016) Crime Scene Photography, Third Edition, Elsevier Inc. California

Ennin and Mensah (2019) Cybercrime in Ghana and the Reaction of the Law Journal of Law, Policy and Globalization, ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)

Eoghan Casey (2011) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Elsevier Academic Press, Waltham

Eoghan Casey, Sean Barnum, Ryan Griffith, Jonathan Snyder, Harm van Beek and Alex Nelson, The Evolution of Expressing and Exchanging Cyber-investigation Information in a Standardized Form. In Handling and Exchanging Electronic Evidence Across Europe, pages 43–58. Springer, 2018.

Etges with Sutcliffe, (2011). An Overview of Transnational Organized Cyber Crime. Journal of Digital Forensic Practice

Faqir (2013) The use of Technology of Global Positioning System (GPS) in Criminal Investigation and Right to Privacy under the Constitution and Criminal Legislations in Jordan: Legal Analysis Study.

Flick, U. 2011. Introducing research methodology: A beginner's guide to doing a research project. London: Sage.

Fombad, C.M. 2017. Comparative Research in Contemporary African Legal. Journal of Legal Education, Volume, 67(4)

Foreign Affairs and International Trade of Canada (2006)

G. Kessler, (2011) "Judges' Awareness, Understanding and Application of Digital Evidence," Journal of Digital Forensics, Security and Law, vol. 6, no. 1, Article 4,

Gardner and Anderson (2011) Criminal Law 11th Edition Cengage Learning

Gino (2003) Basic Police Powers: Arrest and Search Procedures 3rd Edition

Goddard, W. & Melville, S. 2004. Research methodology: An introduction. 2nd edition. Cape Town: Juta.

Grabosky, P., Smith, R., & Dempsey, G. (2001). Electronic Theft: Unlawful Acquisition in Cyberspace. Cambridge, UK: Cambridge University Press.

Harvey D. 201, Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age. Hart Publishing, Oxford

Holt T, Bossler A.M. with Siegfried-Spellar K.C. 2015. Cybercrime and Digital Forensics. Routledge, London and New York

Ian J. L. 2015. Information technology law. Oxford University Press. London

international edition. 10th edition. USA: Pearson

Jarrett, M. H. with Bailie, M.W. 2009. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. www.justice.gov/criminal/cybercrime/

John N. Ferdico , Henry F. Fradella , (2015) Criminal Procedure for the Criminal Justice Professional. Cengage Learning; 12th edition

John N. Ferdico , Henry F. Fradella , Christopher D. Totten (2012) Criminal Procedure for the Criminal Justice Professional. Cengage Learning; 11th edition

John R. Vacca (2013) Computer Forensic: Computer Crime Scene Investigation Second Edition.

Jones and Winster 2017. Forensic Analysis on smart phones using mobile Forensic Tools International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 8 (2017), Research India Publications.

Kelly, K. 2016. From encounter to text: Collecting data in qualitative research (287-319) In Terre Blanche, M., Durrheim, K. & Painter, D (ed.) 2016. Research in practice: Applied methods for the social sciences. 2nd edition. Cape Town: Juta.

Kerr, O.S. (2013), Computer Crime Law. St. Paul, MN: West Academic.

Khaldi, K. 2017. Quantitative, qualitative or mixed research: which research paradigm to use. Journal of educational and social research, 7(2):15-24.

Kohn, M., Olivier, M.S. and Eloff, J.H.P., 2006. Framework for a Digital Forensic Investigation. In Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa, pp. 1–7.

Kshetri, Nir (2006), ―The Simple Economics of Cybercrimes‖, IEEE Security and Privacy, January/February, 4 (1), 33-39.

Kumar, R. 2014. Research methodology: A step- by – step guide for beginners. 4th edition. London: Sage.

Larry E. and Lars E. 2012. Digital Forensic for Legal Professionals: Understanding Evidence from the courtroom. Academic Press.

Leedy, P.D. with Ormrod, J.E. 2013. Practical research: Planning and design. 10th edition. Upper Saddle River, NJ: Merrill Prentice-Hall.

Leedy, P.D. with Ormrod, J.E. 2014. Practical research planning and design: Pearson new international edition. 10th edition. USA: Pearson

Locke, L.F., Spirduso, W.W. & Silverman, S.J. 2014. Proposals that work: A guide for planning dissertations and grand proposals. California: SAGE.

Lune, H., Pumar, E.S. & Koppel, R. 2010. Perspectives in social research methods and analysis: A reader for sociology. United Kingdom: Sage.

Lydia Nkansah and Victor Chimbwanda, 2016 'Interdisciplinary Approach to Legal Scholarship: A Blend from the Qualitative Paradigm' 3(1) Asian Journal of Legal Education 56, 59–60

M.O Hewling 2013. Digital forensics: an integrated approach for the investigation of cyber/computer related crimes Name: dissertation submitted to the University of Bedfordshire.

Maat S.2009. Cybercrime: A comparative Law Analysis', University of South Africa

Madzivhanḓila 2019. an analysis of the role of south african police service railway policing in crime prevention in south Africa. PhD thesis, University of South Africa.

Maghaired A. M 2012. Combating Cyberterrorism: The Response from Australia and New Zealand in James Veitch (ed) International Terrorism New Zealand Perspective.

Maghaired A. M. 2005. Shariah Law, Cyber – Sectarian Conflict and Cybercrime: How can Islamic Criminal Law Respond to Cybercrime. International Journal of Cyber Criminology

Maria Karyda and Lilian Mitrou 2007. Internet Forensic: Legal and Technical Issues. 2nd International Workshop on Digital Forensic and Incident Analysis.

Marras H.,2015 computer Forensics. Cybercriminals, Laws, and Evidence. Jones and Bartlert Learning LLC, Burlington, MA

Marshall, C. and Rossman, G. 2016 Designing Qualitative Research. 6th Edition, SAGE,

Martini, B., and K.-K. R. Choo, 2012. "An integrated conceptual digital forensic framework for cloud computing," Digit. Investig., vol. 9, no. 2,

Martini, B., with Choo, K.-K. R.(2012). An integrated conceptual digital forensic framework for cloud computing. Digital Investigation, 9(2), 71- 80

Mason S 2014. Electronic Evidence 3 ed. LexisNexis.

Mason S with Stanfield 2016. 'Authenticating electronic evidence' in Mason S & Seng D (eds) Electronic Evidence 4 ed (2017) University of London, London

Mason, J. 2014. Qualitative researching. 2nd edition. London: Sage.

McMillan, J.H. with Schumacher, S. 2013. Research in education. Evidence – Based Inquiry: Pearson Education.

McNamara, K. (2012). The high cost of cybercrime. ExpertIP. Retireved from https://allstream.com/study¬-the-high-costs-cybercrime

Meeker, J. (2005). Search and seizure state and federal law Austin, Texas State Bar of Texas.

Merriam-Webster Dictionary (2022)

Michael Donovan Kohn, Mariki M Eloff, and Jan HP Eloff. Integrated Digital Forensic Process Model. Computers & Security, 38:103–115, 2013.

Michael G. Maxfield, Earl R. Babbie. Research Methods for Criminal Justice and Criminology. 7ed (2014). Cengage Learning.

Micheal, S. Maloney 2018, Death Scene Investigation. Procedural Guide. Boca Raton, CRC Press

Miller, M. T. (2011). Crime Scene Investigation. Forensic Science: An Introduction to Scientific and Investigative Techniques.

Ministry of Communication (2014)

Mohamed C., Ashraf D.,and Mohammad A., K., (2015) Cybercrime, Digital Forensic and Jurisdiction, Springer International Publishing, Switzerland.

Mouton, J. 2014. Understanding Social research. Pretoria: Van Schaik.

National Institute of Justice ((2008) Electronic Crime Scene Investigation guides for first responders

Nieman (2009) Cyberforensics: Bridging the Law/ Technology Divide. *Journal of Information, Law & Technology (JILT)*

Obuobisa Y.A. (2019) Challenges faced regarding cybercrime and the rule of law in cyberspace from the perspective of a prosecutor in Ghana.

Osterburg, J.W., with Ward, R.H. 2010. Criminal investigation: A method for reconstructing the past. 6th edition. New Jersey, USA: LexisNexis.

Palmbach and Breitinger (2020).Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability. Forensic Science International Elsevie.

Palmer, G., 2001. A Road Map for Digital Forensic Research. In First Digital Forensic Research Workshop, Utica, New York. pp. 27–30.

Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, Hossein Taji (2016) Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Faculty of Law, The National University of Malaysia (UKM) Bangi, Malaysia.

Pearson Merrill Prentice Hall.

Petersen, K. and Gencel, C. (2013). Worldviews, research methods, and their relationship to validity in empirical software engineering. Joint Conference of the 23rd International Workshop on Software Measurement.

R. Leigland and A. Krings, (2004) "A Formalization of Digital Forensics," International Journal of Digital Evidence, vol. 3, no. 2, 2004.

Ravitch, M. and Riggan, M. 2012 How Conceptual Frameworks Guide Research. SAGE Publications.

Regan, K. (2006). FBI: Cybercrime Causes Financial Pain for Many Businesses, tech news world.

Richard, Saferstein. 2019, Forensic Science. From the Crime Scene to the Crime Lab. 4th edition, New Jersey Pearson Education Inc.

Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., and Debrota, S., 2006. Computer Forensics Field Triage Process Model. In Proceedings of the conference on Digital Forensics, Security and Law (CDFSL 2006). Association of Digital Forensics, Security and Law, p. 27.

Rogers, M., 2006. DSCA: A Practical Approach to Digital Crime Scene Analysis. In Information Security Management Handbook, Fifth Edition, Volume 3. pp. 601–614.

Rolando del Carmen and Craig Hemmens. 2017. Criminal Procedure: Law and Practice. 10th Edition

Rolandon del Carmen 2013. Criminal Procedure: Law and Practice. Wadsworth.

Ross M. and Donna K. (2019) Practical Crime Scene Processing and Investigation (Practical Aspects of Criminal and Forensic Investigations), Third Edition, Taylor and Francis Group LLC Baton Raton, Florida.

Ruan K, Joe Carthy, Tahar Kechadi, and Ibrahim Baggili. Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: An Overview of Survey Results. Digital Investigation, 10(1):34–43, 2013.

Sady (2012), Developments in Federal Search and Seizure Law. Available from: http://or.fd.org/search%20and%20seizure.pdf

Satola and Judy 2011 “Convention on Cybercrime, Council of Europe”

Satola and Judy,(2011) Convention on Cybercrime, Council of Europe. William Mitchell Law Review

Scanlon, M., 2016. Battling the Digital Forensic Backlog through Data Deduplication. In Proceedings of 6th IEEE International Conference on Innovative Computing Technology (INTECH 2016), Dublin, Ireland, pp. 10-14.

Scheb and Scheb (2011:448) Criminal Law and Procedure 7th Edition wadsworth

Seale, C. 2004. Social research methods: A reader. London: Routledge.

Sibanda, O. 2015 Public interest considerations in the South African anti-dumping and competition law, policy, and practiceInternational Business & Economics Research Journal (IBER). Volume 14, issue 5

Silverman, D. 2014. Interpreting qualitative data. 5th edition. London: Sage.

Smith, Grabosky, and Urbas (2012) Cybercriminal on Trial, Cambridge: Cambridge University Press,

Sneha C Sathe and Nilima M Dongre. Data Acquisition Techniques in Mobile Forensics. In 2018 2nd International Conference on Inventive Systems and Control (ICISC), pages 280–286. IEEE, 2018

South Africa Bank Risk Information Centre (SABRIC) 2018)

South Africa. 1995. Police Service Act 68 of 1995. Pretoria: Government Printer.

South Africa. 2002a. Electronic communication and transactions Act 25 of

South Africa. 2002b. Regulation of interception of communication and provision

South Africa. 2015. Scam targets Winnie to lure victims. Sowetan. Online:

South African Police Annual Report. 2015. Pretoria: Division Human Resource Development. SAPSAR 2014/2015.

South African Police Annual Report. 2016. Pretoria: Division Human Resource Development. SAPSAR 2015/2016. 96

South African Police Annual Report. 2017. Pretoria: Division Human Resource Development. SAPSAR 2016/2017.

South African Police Annual Report. 2018. Pretoria: Division Human Resource Development. SAPSAR 2017/2018.

Susan W.B.2010. Cybercrime: Criminal Threats from Cyberspace. Prager, Santa

Swason, Chamellin, Territo and Taylor (2019) Criminal Investigation 12th Edition McGraw Hill

Symantec Coporation (2019)

Symantec Corporation (2017)

T. Padma and K.P.C. Rao, Legal Research Methodology, (1stAsia Law House, Hyderabad 2011)

Tavakoli, H. 2012. A dictionary of research methodology and statistics in applied linguistics. Iran: Rahnama press. Elsevier Academic Press London.

Thanh, N.C. & Thanh, T.T.L. 2015. The interconnection between interpretivist paradigm and qualitative methods in education. American journal of educational science, 1(2):24-27.

The Institute of Company Secretaries of India (2016).

Thomas J., Holt 2018. Regulating Cybercrime through Law Enforcement and Industry Mechanisms. America Academy of Political and Social Science.

Thomas J.H and Adam M. B. 2016. Theory and prevention of technology-enabled offenses (Crime Science Series), Routledge, New York.

Thomas K. Clancy. 2014. Cyber Crime and Digital Evidence: Materials and Cases. San Francisco. LexisNexis

Thomas, G. 2013. How to do your research project: A guide for students in Education and applied social sciences.2nd edition. London: Sage. Thomson Learning Inc. California.

Thomas, J. Gardner & Terry, M. Anderson. 2015, Criminal Evidence. Principles and Cases. Boston Cengage Learning

United Nations Office on Drugs and Crime (UNODC) 2013),

United Nations Office on Drugs and Crime (UNODC) 2020),

Urbas and Choo K (2008) Resource materials on technology-enabled crime.Technical and background papers series no.28. Canberra: Australian Institute of Criminology.

Van Baar, R.B., van Beek, H.M.A. & van Eijk, E.J., 2014. Digital Forensics as a Service: A Game Changer. Digital Investigation.

TABLE OF CASES

Atkins v The Lord Chancellor [2014] EWHC 1387 (QB)

Ashcroft v. Free Speech Coal, 535 U.S. 234, 249-50 (2002)

Arizona v. Hicks 480 U.S. 321 (1987)

Bumper v. North Carolina, 391 U.S.543, 550 (1968).

United States v. McKeever, 169 F. Supp. 426 (S.D.N.Y. 1958)

Camden London Borough Council v. Hobson

Castle v. Cross [1984] 1 WLR 1372,

Crinion v IG Markets Ltd [2013] EWCA Cir. 587,

Chapman v. United States, 365 U.S. 610, 81 S.Ct. 776, 5 L.Ed.2d 828 (1961).

Chimel v. California (395 U.S. 752 (1969)

Control Magistrate, Durban v AZAPO,29

United States v. Carey

Clinton v. Virginia, 377 U.S. 158 (1964)

Coolidge v. New Hampshire 403 U.S. 443 (1971)

Commonwealth v Monzon 744 N.E.2d 1131 (2001)

Daubert v. Merrell Dow Pharmaceuticals,Inc. 509 U.S. 579 (1993)

Director of Public Prosecutions (DDP) v. McKeown

Director of Public Prosecution v Sutcliffe, (2001)

Director of Public Prosecutions (DDP) v. Jones

Franks v. Delaware, 438 U.S. 154 (1978).

Frye v. United States 293 F. 1013 (D.C. Cir. 1923)

Glenn Whittle v The Commissioner for Her Majesty's Revenue & Customs (2014)

Griffin v. Wisconsin, 483 U.S. 868 (1987).

Harris v. United States, 390 U.S. 234 1968

Horton v. California, 496 U.S. 128 (1990)

Illinois v. Gates, 462 U.S. 213, 238 (1983).

Illinois v. Rodriguez, 497 U.S. 177, (1990)

In Davis v. Gracey, 111 F.3d 1472, 1480 (1997),

In Maryland v.Garrison, 480 U.S. 79 (1987),

Intercity Telecom Limited and Anor v. Sanjay Solanki. 2 Costs LR 315, (2015)

Katz v. United States, (1967)

Katz v. United States, 389 U.S. 347 (1967),

Kyllo v. the United States, 533 U.S.27, (2001)

Kennedy v. Baker

Knox v. States of Indiana (93 F.3d 1327),

Lorraine v. Markel Am. Ins.Co., 2007 WL 1300739 (D. Md., May 4, 2007

Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 544 (2007)

Lord Advocate v Blantyre

Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, 545 U.S. 913 (2005),

Marcus v. Search Warrant, 367 U.S. 717 (1961)

Magajane v. the Chairperson of the North West Gambling Board (2006)

Minister for Safety and Security v. Van Der Merwe and Others (2011)

Malley v. Briggs, 475 U.S. 335.

Michigan v. Summers, 452 U.S. 692 (1981).

Mollet v State 939 P.2d 1 (Okla.1997) 743).

Nardinelli et al v. Chevron

New Jersey v. T.L.O. 469 U.S. 325 (1985)

Naidoo and Another v Minister of Law and Order and Another 1990

Ornelas v the United States 517 U.S. 690, 696 (1996).

Olmestead v. United States, 277 U.S. 438 (1928),

Queen v. Luqman Farooq (2019)

R v. Shephard (1988) 86 Cr App R 47

R v Bowden 2 All ER 418 the English Court of Appeal

R. v. Smith; R. v. Jayson 1 Cr App R 13, CA,

R v. Fellows; R v. Arnold 1 Cr App R 244; 2 All E.R. 548

R v. Spiby (1991) Crim. L.R. 199 (C.A.Cr.D.)

R v Peirson [2014] QSC 134,

R v Madhub Chunder Giri Mohunt

Roads and Traffic Authority v. McNaughton

Gates Rubber Co v. Bando Chemical Industries Ltd 9 F.3d 823 (10th Cir. 1993)

Re Grand Jury Investigation Concerning Solid State Devices, Inc. v. United States (130 F.3d 853, 857),

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)

R v Fowden and White (1982) Crim L R 588

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)

Schneckloth v. Bustamonte 412 U.S. 218, 228 (1973)

shadwick v. City of Tampa, 407 U.S. 345 (1972)

Coolidge v. New Hampshire 403 U.S. 443 (1971)

Arizona v. Hicks 480 U.S. 321 (1987)

Horton v. Californi 496 U.S. 128 (1990).

shadwick v. City of Tampa, 407 U.S. 345 (1972)

silverman v. United States, 365 U.S. 505 (1961)

Sectrack NV v. Satamatics Ltd (2007)

Solid State Devices, Inc. v. United States 130 F.3d 853, 857

State of North Carolina v. Robert J. Petrick, (No. COA7-86).

State of Arizona v. Dean, 206 Ariz. 158

State v. Gamage, 340 A. 2d 1,7 (1975)

state v. Hendricks, 328 N.E. 2d 822 (1974).

state v. Vitale, 530 P2d 394 (1975),

State v. Brousseau

State v.Valentine, 504 P.2d 84 (1972)

Stoner v. California, 376 U.S. 483, (1964).

Trend Finance (Pty) Ltd and Another v Commissioner of SARS and Another (2005)

Texas v. Johnson, 491 U.S. 397,414 (1989).

United States v. Jacobsen, 466 U.S. 109, 113 (1984)

United States v. Adjani, 452 F.3d 1140, 1148, 9th Cir. (2006).

United States v. Adjani, 452 F.3d 1140, and 1145-46 9th Cir. (2006)

United States v. Arnold 454 F. Supp. 2d 999, 1994 ([C.D. Cal (2006),

United States v. Bailey, 272 F.Supp. 2d 822, (D. Neb.2004),

United State v. Sandoval vargas, 490 U.S. 854 F.2nd 1132, 1134 (1998)

United States v. Blas, (1990 WL 265179)

United States v. Banks, 124 S.Ct. 521. (2003)

United States v. Reyes, (922 F. Supp. 818, 834 1996)

United States v. Bennett, 363 F.3d 947, 953 (9th Cir. 2004)

United States v. Bunty, 2008 Wisconsin v. Schroeder, 1999 United States v. Gray, 1999.

United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988)

United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003)

United States v. Simnons, 206 F.3d 392 2000

United States v. Couch, 688 F2d 599, 604 [9th Cir. 1982])

United States v. David, 756 F. Supp. 1385 (1991),

United States v. Davis (482 F.2d 893 9th Cir. 1973),

United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir. 1970).

United States v. Elliott, 893 F2d 220 (9th Cir. 1990),

United States v. Flores-Montano, 541 U.S.149, 152-153 (2004).

United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999).

United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007)

United States v. Ganias (2016) Riley v. California (2014)

United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008)

United States v. Grubbs, 547 U.S. (2006),

United States v. Hamilton, 413 F.3d 1138, 1142-43 (10th Cir. 2005)

united States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000),

Beck v. Ohio 379 U.S. 2d 223 144, 145 (1964)

United States v. Kassimu, 2006 WL 1880335 (5th Cir. Jul. 7, 2006)

United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) “

United States v. Kilbride, 584 F.3d 1240 (9th Cir.2009)

United States v. Kim (2015)

United States v. Kow, 58 F.3d 423, 427 9th Cir. (1995).

United States v. Lattimore, 87 F.3d 647, 651 (4th Cir. 1996)

United States v. Laury, 985 F.2d 1293 (5th Cir. 1993),

United States v. Salcido, (506 F.3d 729, 733 2007)

United States v. Roman,

United States v. Lckes 393 F3d, 501,503 (4th Cir. 2005)

United States v. Wong, (334 F.3d 831, 838 9th Cir.)

United States v. Leary, 846 F.2d 592, 600-04 (10th Cir. 1988)

United State v. Sandoval vargas, 490 U.S. 854 F.2nd 1132, 1134

United States v. Martin, 426 F. 3d 3 (2005);

United States v. Martin, 426 F. 3d 3 (2d Cir. 2005);

United States v. Matlock, 415U.S. 164, 171.

United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001)

United States v. Meyer, 417 F:2d 1020 (8th Cir. 1969).

United States v. Montoya de Hernandez 473 U.S 531, 538 [1985]

United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009)

United States v. Pena, 143 F.3d 1363, 1368 (10th Cir. 1998).

United States v. Percival, 756 F.2d 600 (7th Cir. 1985)

United States v. Principe, 499 F.2d 1135 (1st Cir. 1974),

United States v. Robinson, 414 U.S. 218 [1973]).

United States v. Rodriquez, 628 F.3d 1258 (11th Cir.2010)

United States v. Ross, 456 U.S. 798, 820-21 (1982

United States v. Simons, 206 F.3d 392 (2000)

United States v. Turner (1999)

United States v. Wagers, 339 F Supp. 2d 934 (E.D. Ky.2004).

United States v. Wagner, 989 F2d 69 (2d Cir. 1993),

United States v. Washington, 498 F.3d 225, 230-31 (4th Cir. 2007),

United States v. Williams, 553 U.S. 285 (2008)

United States v. Thevis 469 F.Supp.490(D.Conn1979)

Vale v. Louisiana, 399 U.S. 30

Valdez v. State, 476 A. 2d 1162 Md. (1984)

Wolpe v Officer Commanding South African Police

Wilson v. Arkansas (514 U.S. 927 (1995),

Wilson v. Layne, 526 U.S. 603 (1999),

Wyoming v. Houghton, 526 U.S. 295, 307 (1999)

Ybarra v. Illinois, 444 U.S. 85 (1979).

LIST OF LEGISLATION AND INSTRUMENTS

Civil Evidence Act 1995

Civil Proceedings Evidence Act 25 of 1965.

Commonwealth Evidence Act 1995

Computer Evidence Act 57 of 1983

Computer Misuse Act 1990

Crimes Act 1914

Criminal Offences Act 29 of 1960

Data Protection Act 843 of 2012

Electronic Communication Act 775 of 2008

Electronic Communication and Transactions Act 25 of 2002

Electronic Communication Privacy Act of 1996 (ECPA)

Electronic Transaction Act 772 of 2008

Evidence Act 1975 (N.R.C.D 323)

Evidence Act 1975 (N.R.C.D 323)

National Communication Authority Act 524 of 1996

Non-Solicited Pornography and Marketing Act of 2003

Security of Critical Infrastructure Act 2018 (Cth);

South Africa Cybercrimes Act 19 of 2020

Telecommunications (Interception and Access) Act 1979 (Cth)

U.S. SAFE WEB Act of 2006, CAN-SPAM Act

US Federal Rules of Evidence

LIST OF FIGURES

LIST OF ANNEXURES

Impact Writing and Editing Solutions

_____

Professional Communication Hub
ImpactWritingEdits@gmail.com

22 November 2022

To Whom It May Concern,

I hereby confirm that I undertook the editing and proof-reading for the thesis titled:

"**AN EXPLORATION OF VIRTUAL CRIMINAL INVESTIGATIONS IN GHANA: LEGAL ISSUES AND CHALLENGES**"

by student Augustine Amoako (student No: 46473742) for a qualification registered at the College of Law, University of South Africa.

The candidate remains responsible for the scholarly merit of his work.

Issued by:

O Stephens, BJURIS, LLB, LLM, LLD

Member: Professional Editor's Guild – South Africa (PEG-SA)

TURN-IT-IN SIMILARITY INDEX REPORT