WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Web Based Forensic Investigative Model for Effective Crime Tracking and Report System in Nigeria

Chilaka K. J.[a], Oliver E. O.[a], Agbakwuru O. A.[a], Chilaka U.L.*

[a,*]Department of ComputerScience, Faculty of Physical Science, Imo University, Owerri, Nigeria
[*]Department of Computer, Kingsley Ozumba Mbadiwe University, Ogboko, Imo State, Nigeria

ABSTRACT :

Digital devices have become an integral part of our everyday life, hence their involvement in almost all crimes committed around the world. The involvement of digital devices in crimes poses new challenges for investigators such as identification and collection of digital evidence from a crime scene, analyzing and presenting digital evidence in a manner that will be admissible in a court of law. The aim of this work is to develop a digital forensic model that will be effective in crime investigation in security agencies. The motivation came because of the lack of standard digital forensic model to guide the investigator through the process of investigation. The methodology used was Object Oriented Analysis and Design Methodology (OOADM). The new system will be implemented and programmed using PHP and MYSQL as database. The proposed system will help in evaluation of model which shows that is capable of tracking crime in the Country via the web application Programming Interface.

Keywords: Digital device; crime; investigation; forensic; bank; evidence and identification

Introduction :

Digital forensics can aid an investigator in the analysis of criminal activities. A digital forensics investigator may review deleted files, hidden files, emails, short message service (SMS), and multimedia files to track criminal activities. Every online activity leaves a trace that can be followed by a seasoned investigator. Digital forensics can aid an investigator in locating a suspect. People often use their laptops, tablet, smart phone, and smart watch to navigate the online map and even check in to their favorite spot on Face book. Hence, an investigator may review someone's GPS history to determine their location. However, digital forensics is a new technology in Nigeria. Digital forensics is a collection of pre-defined processes or tasks used in the course of a criminal investigation, with some technical implementation specifics shared with traditional forensics for managing and collecting technical evidence information (Arpita,et al, 2023). Although a variety of digital forensic investigation frameworks have been offered by numerous researchers and practitioners. The inquiry procedure becomes hard due to numerous technical and legal details. To break down the technological barriers that exist between investigators, information technologists, and legal practitioners, the researcher must present a technical-independent framework that can bring all of these duties together. This study emphasized a critical principle of digital forensics investigations (Obtaining authorization, documentation, information flow, preservation, collection of evidence, and evidence analysis). Based on this technique, the author defines five questions for digital forensic inquiry. An expert in digital forensics A digital forensics investigation algorithm is created by incorporating these five sets of queries

In the review done by Radina and Katrin (2023) proposed a formal reliability validation enabling framework (RVEF) for evaluation of digital forensics in criminal investigations. The RVEF is informed by examined theoretical and conceptual gaps between law and digital forensics related to reliability and validation. Identified are validation criteria and validation testing techniques for digital forensics as well as their limitations and challenges. The proposed RVEF aims to satisfy the objective for documenting the chain of evidence and custody as standard process. It is a generic and extensible approach to create a formal procedure for documentation of reliability information at three levels: technology, method, and application. For each level reliability criteria are compared against international digital forensic standards, guidelines, and best practices in order to elaborate concrete minimum documentation requirements necessary to enable reliability validation by law enforcement. The framework aims to increase accountability, reliability testing, and machine-human error mitigation in digital forensics. It can also serve judges and defences lawyers to cross-examine the forensic report in a formalized process, access the proportionality of the investigation measures, and potential risks from the inappropriate use of technology.

Nigeria experienced 3,500 cyber-attacks with over 70 percent success rate and a loss of $450 million between 2015 and 2016 (Umoru, 2017). We are seeing significant interest by cybercriminals in leveraging ICT capabilities to further their cause. For example, the Independent National Electoral Commission (INEC) was hacked and taken over on the day of the 2015 presidential election (Onwubiko, 2018). Consequently, it is no exaggeration to say that digital devices have become an integral part of our everyday lives (Jacob, 2014). In the course of using these digital devices, we leave behind a lot of information and insights into our character, behavior, and plans on our digital devices (prudential associates, 2016). The data left behind on a digital device generally can be used in investigations of any nature, both civil and criminal. Digital forensics can aid an investigator in the analysis of criminal activities. A digital forensics investigator may review deleted files, hidden files, emails, short message service (SMS) , and multimedia files to

track criminal activities. Every online activity leaves a trace that can be followed by a seasoned investigator. Digital forensics can aid an investigator in locating a suspect. People often use their laptops, tablet, smart phone, and smart watch to navigate the online map and even check in to their favorite spot on Face book. Hence, an investigator may review someone's GPS history to determine their location. However, digital forensics is a new technology in Nigeria. It became acceptable and applicable in Nigeria after the enactment of the Nigerian Evidence ACT 2011. Before 2011, digital evidence was not out rightly admissible as evidence in the Nigerian Courts due to loopholes in the law and case law controversies. The application of digital forensics in the investigation of cybercrimes was further given a boost under the enactment of the Nigerian Cybercrimes (Prohibition, Prevention, etc,) Act 2015, which came into force in May2015. Consequently, security and law enforcement agencies realized the need for digital forensics in the fight against crimes. A statement released by the former Inspector General of Police (IG), Solomon Arase, made it clear that the establishment of a digital forensics laboratory will help the force to tackle the challenge of identity conflict and denial of evidence by suspects in the court of law (Okakwu, 2016). With this in mind, a digital forensics laboratory was established in Abuja for the Nigerian Police force in 016 (Okakwu, 2016). Most security and law enforcement agencies are not using digital forensics in their investigation, hence the Economic and Financial Crimes Commission (EFCC) has pledged to provide forensics assistance to agencies involved in complex crime investigation (Ogune, 2018). In Nigeria today, EFCC is seen as the number one agency in the use of digital forensics in the investigation of crime. However, they still lack when placed on a global scale with other security and law enforcement agencies around the world. They need a competent computer forensics expert to win high profile cases in an anti-graft fight. The President of Nigeria, Muhammadu Buhari, charged the agency to stop losing cases (Oluka, 2017). Most cases being lost in the Nigerian Courts are arguable as a result of the agencies' lack of use of digital forensics and the non-application of a standardized and acceptable universal procedure. Not only the EFCC, according to Chijioke (2013), a total of 1,072,026 cases were recorded between 1996 and 2000 by the Nigerian Police Force, only 43.1percent (462,058) cases were prosecuted while 50.5 percent (540,899) were either under-investigated or closed for lack of evidence (Soyombo,2005). According to Otu (2018), the Nigerian Police Force has failed in the use of forensics in the investigation of crimes. Irrespective of the application of digital forensics by some security and law enforcement agencies in Nigeria in the investigation of crimes, there is a need for more to be done in the area of standardizing the application of digital forensic to bring all the investigators on the same plane. The EFCC and Department of State Services (DSS)are ahead of others in the use of digital forensics, which calls for regularization to bring all the security and law enforcement agencies to the same level. Digital forensics is not regulated in Nigeria which is evident in the high loss of court cases by the agencies. An example of a case that was not successfully prosecuted is the EFCC vs James Ibori case (BBC News, December 17, 2009) The EFCC was not able to successfully prosecute James Ibori because the evidence they had against him was not admissible by the court, but he was later successfully prosecuted and jailed in the United Kingdom (UK) for the same offense (Sahara Reporters, New York, May 04, 2012). Not having a regulatory body regulating digital forensics in Nigeria is the root cause of inconsistencies in the investigation processes. A regulating body will harmonize and formalize the investigation process in Nigeria, thereby making it easy for all the security and law enforcement agencies to follow the same process while using digital forensics for crime investigation. Notably, the benefits of the regulation of digital forensics investigation cannot be overemphasized when juxtaposed against the USA, UK, India, and some other countries that regulate digital forensics. USA regulates digital forensics through a code of ethics established by various certification entities or professional digital forensics societies such as the American Academy of Forensics Science (AA FS) (American Academy of Forensics Science [AAFS], 2013), American Board of Criminalities (ABC) (American Board of Criminalities [ABC], 2013), California Association of Criminalists (CAC) (California Association of Criminalists [CAC],2010),High Technology Crime Investigation Association(HTCIA),etc. They outline the ethical requirements for digital forensics. India through the Ministry of Electronics and Information Technology (MEIT) provides a guideline for digital forensics. Sub-agencies and autonomous societies of MEIT such as India Computer Emergency Response Team (ICERT), Cyber Appellate Tribunal (CAT),Centre for Development of Advance Computer(C-DAC), ensures that investigators and prosecutors adhere to the code of ethics for the practice of digital forensics (Rachiyta, 2015). The UK has one of the best-documented standards for digital forensics that has been adopted by several other nations (Forensics Science Regulator [FSR] (2014). Association of Chief Police Officers (ACPO) of England, Wales, and Northern Ireland developed a guide named: ACPO Good Practice Guide for Digital Evidence (Janet, 2012). This guide is for both law enforcement agents and all that assists in investigating cyber security incidents and crime. The guide is updated from time to time according to legislative and policy changes. Currently, it is having five (5) versions (Janet, 2012). Regulation brings both investigators and prosecutors on the same plane of best practices and a good code of conduct practiced nationwide. A good example is the ACPO practice guide, which makes it possible for an investigator in England to follow the same standard with an investigator in Northern Ireland well as Wales. The effect is, all the investigators will produce the same result with the same standard. Unfortunately, different security and law enforcement agencies in Nigeria have different standards for the investigation of crimes, hence one cannot categorically say that Nigeria has a digital forensics model used by all the security and law enforcement agencies. Lack of a generally acceptable digital forensics model poses great challenges for crime investigation and prosecution in Nigeria. Discharge and acquittal of defendants brought before courts of competent jurisdiction is a major challenge of not having a digital forensics model. Cases are being dismissed and defendants discharged not because all the defendants are innocent, but because of lack of admissible evidence and shoddy investigations. The admissibility of digital evidence is based on the procedure (digital forensics model) used for the acquisition of such evidence. When the right procedure is not followed, such evidence will be thrown out, hence if there is no evidence to prosecute an accused person, he/she will be discharged and acquitted.

(Farkhund et al, 2023) Small-scale digital devices like smartphones, smart toys, drones, gaming consoles, tablets, and other personal data assistants have now become ingrained constituents in our daily lives. These devices store massive amounts of data related to individual traits of users, their routine operations, medical histories, and financial information. At the same time, with continuously evolving technology, the diversity in operating systems, client storage localities, remote/ cloud storages and backups, and encryption practices renders the forensic analysis task multi-faceted. This makes forensic investigators having to deal with an array of novel challenges. The study reviews the forensic frameworks and procedures used in investigating small-scale digital devices. While highlighting the challenges faced by digital forensics, they explore how cutting-edge technologies like Blockchain, Artificial Intelligence, Machine Learning, and Data Science may play a role in remedying concerns. The review aims to accumulate state-of-the-art and identify a futuristic approach for investigating SSDDs.

Another challenge is the time spent in crime investigation. With a digital forensics model, investigators do not need to spend unnecessary time since he or she will be guided on what to do and how to do it (NITDA, 2014). Again, it has resulted to conflicting results and evidence emanating from digital forensics examinations by forensics units and experts within the Nigerian Law Enforcement community .Because cases are being thrown out, accused persons are discharged, conflicting forensics reports, and investigations are prolonged due to lack of a digital forensics model (Micheal, 2015). A digital forensics model is required for effective investigation and prosecution of crimes in Nigeria. This work starts with an introduction of the topic under consideration by demonstrating the impact of ICT on the lives of Nigerians specifically and globally and how it has aided the proliferation of crimes. It portrays the slow embracement of the application of digital forensics by security and law enforcement agencies and the consequent challenges. Thereafter, the work critically and from a comparative posture examines the general tackling of crimes through the application of digital forensics and how a general acceptable model and standardization could aid or mar investigations. In this regard, the work advocates for a digital forensics model that would be generally used by all investigators including government and private investigators. Thereafter, considering the necessity of credible evidence and the impact digital evidence can make in criminal proceedings, a critical examination on the effectiveness or otherwise of forensics in criminal adjudication before the Nigerian Courts are made.

This research primarily focuses on the problem of forensic investigators is rooted in the scale of the devices of forensic interest, relevance, and hazy/edgeless network boundaries (Perumal et al., 2015). Another gap, in addition to physical inaccessibility, is the collection of evidence from cloud storage and data centres. Since data may be stored in different locations/nations, the issue of multiple jurisdictions must also be taken into consideration (Zulkipli et al. 2017). Also, to enable the correlation of incidents across various log sources, it is crucial to guarantee that prospective forensic data sources are time-stamped. All of the devices' time must be synchronized and securely managed. Digital evidence is extremely fragile and is easily altered, removed, or tampered with (Farkhund et al. 2023). There is a danger of gadgets remotely shutting down or evidence being overwritten. As an option to deal with this issue, the majority of devices save their data in the cloud. : Law enforcement agencies uses traditional form of crime investigations for collection, analysis, and preparation of the evidence for legal proceedings; no standard digital forensic model to guide the investigators through the process of investigation and real time crime tracking and reporting. and no central crime reporting database repositories for Law enforcement agency that contain information of Nigerian citizens.

In most trial, the respondent was discharged and acquitted on all counts. This is a case where the application of a digital forensic investigation by the EFCC would have aided the court in answering the questions posed by it based on real time evident and crime report to the law enforcement forensic database. Another peculiar challenge is the inadequate use and device connectivity within the digital forensic space (Farkhund et al. 2023), by the lead investigator who testified in the matter. In most cases of crime evidence gathering and investigations, the respondent's smart phone, e-mail, internet facility, and hard drive may not presented before any forensic expert for forensic examination to link the respondent to the commission of the crime. The problems that formed these research are based on the traditional crime investigations system that have become ineffective not just in Nigeria but in the world over, resulting in a paradigm shift to digital forensics. However, in Nigeria, there is This has resulted in prolonged investigation and prosecution of criminal cases and conflicting results from digital forensic suits and experts within the Nigerian law enforcement community.

The primary aim of this research is to develop a digital forensic investigative model for effective tracking and reporting crime in Nigeria. The specific objectives are: to develop an investigative framework for digital forensic crime collection, analysis and preparation; to analyzed the reported crime using a statistical analysis ; To develop a crime based database for possible crime log and tracking for Law enforcement agencies such EFCC, Nigeria Police Force, NDLEA and ICPC; to develop a real time web based application for Nigeria citizens, investigator and law enforcement agencies for immediate crime reporting at the point of crime incidents. This research work centered on digital forensic model for investigating crime and reporting. This research takes its step by reviewing the existing forensics model in Nigeria crime investigation, tracking and reporting and introduced a digital forensics model based real time via web application for ease reporting and collating crime incidents. The primary focus also on this research is to provide ease accesses for crime reporting using digital device for accessing reporting system to crime activities for Law enforcement agencies

Related Works :

As technology level documentation assures validation of tools and specific functionality of the automated setup which is employed in the investigation task. A methodology level documentation provides proof that an accepted scientific procedure, and standardized sequence of steps is followed to provide reliable results. It includes method, algorithms, and feature selection and detailed description of dataset, experiment setup and preprocessing for input. Radina and Katrin (2023) At the application level, it was identified that the examiner's interaction with the method and tool as well as subjective measurements must be traceable and justified according to the concrete forensic task. The RVEF is general and needs to be elaborated and tested further. Nevertheless, the added value of RVEF is that it enables the gradual development of techno-legal standards for reliability as it facilitates any type of testing on any stage of the evidence processing. Further, it can be used by LEAs to create audit trials of digital forensic actions, which can be studied at large for reducing subjective opinions and assumptions in favour of objective measurements, formal justification of the selected methodology according to the forensic task, and large-scale reliability and error rates studies. Most importantly, the RVEF provides the minimum documentation to secure the opportunity for cross-examination and the challenging of digital evidence on valid grounds in further criminal proceedings. Considering that digital forensics for criminal proceedings requires not only scientific validation, but also proportionality and data protection assessment, the RVEF can serve as a first step to meet these ends as well.

Radina and Katrin (2023) reviewed that digital forensics can reach a level of standardization and validation similar to the classical forensic sciences. However, we identify as major gaps the lack of clear reliability standard and the focus on quality assurance of technology, where methodology and application validation techniques are underdeveloped. As opposed to "one-standard-fits-all" lab requirements, proposed solutions should enable gradual documentation of the methods, tools, and the interaction of examiners across the process in order to enable different types of validation procedures. To support theoretically the development of a reliability standard, we clarified concepts routinely used as a measure for quality assurance in digital

evidence since often they have different nuances in the legal and forensic science domain. The proposed reliability validation framework (RVEF) is a conceptual framework which identifies practical, legal and forensic requirements for evidence reliability and elaborates the related law enforcement requirements in digital forensic processes that needs to be documented in order to meet the high-level criteria. The framework identifies four validation criteria e data set, tool, method, and examiner. The RVEF suggests a model for minimum documentation of three level validation requirements as a first step to address the identified reliability challenges.

Digital Forensic Investigations: Optimal Strategies and Emerging Innovations

According to (Anwaar, 2023) Digital forensic investigations are critical in modern law enforcement, cybersecurity, and legal proceedings. Ensuring digital evidence's accuracy, integrity, and reliability is paramount in these contexts. This review article explores the challenges and best practices associated with quality control in digital forensic investigations and the emerging technologies that are reshaping the field. The article begins by discussing the foundational concepts of quality control in digital forensics, emphasizing the need for standardized procedures, documentation, and validation techniques. It delves into the potential sources of errors and bias that can arise during the acquisition, preservation, analysis, and presentation of digital evidence. It highlights the importance of continuous monitoring and review to mitigate these risks (Anwaar**, 2023).** The review article further examines the evolving landscape of digital forensic tools and technologies advancing quality control efforts. It covers advancements in data acquisition methods, including live forensics and memory analysis, and discusses the role of artificial intelligence and machine learning in automating quality control processes. The integration of Blockchain and cryptographic techniques for ensuring the integrity of digital evidence is also explored. In addition, the article addresses the challenges and opportunities presented by cloud computing, IoT devices, and the proliferation of digital data sources. It emphasizes adaptability and agility in quality control approaches to accommodate the changing digital landscape. Through a comprehensive analysis of established practices and emerging technologies, this review article offers practitioners, researchers, and policymakers' insights into enhancing the reliability and trustworthiness of digital forensic investigations. By adopting robust quality control measures and embracing innovative technologies, the digital forensics community can ensure its findings hold up to scrutiny in the courtroom and beyond.

Cyber-Crime and Digital Forensics

The proliferation of digital and multimedia technologies is influencing the field of digital forensics. Furthermore, the number of cases where digital evidence is relevant to investigations is increasing (Lillis et al, 2016). Due to the huge amount and volume of data available, forensic practitioners find it challenging to analyze digital evidence. Furthermore, the scattered nature of cloud computing makes evidence collection problematic (Neware and Khan, 2018). Law enforcement agencies around the world are experiencing substantial digital evidence backlogs as a result of the rising number of cases requiring digital forensic expertise (Lillis et al, 2016). Criminals, on the other hand, have realized that conducting cybercrime is faster and easier than traditional crime because of technology (Vincze, 2016). In this dynamic context, the purpose of this study is to identify the success factors as well as the key difficulties in digital forensics for law enforcement. This is performed by contrasting and comparing the research community's success elements and challenges with those recognized by digital forensic practitioners. The main goal is to find connections between them. This topic is being offered as part of a collaboration agreement between the University of Skövde and the Swedish Police's Forensic Department in Västra Götaland to conduct forensic methods research. A systematic literature review was planned, with current and available scientific literature linked to the topic of interest published between 2015 and 2021 serving as the major source of information. Similarly, the results of a survey of Swedish Police forensic practitioners will be used to triangulate the findings of the systematic literature review.

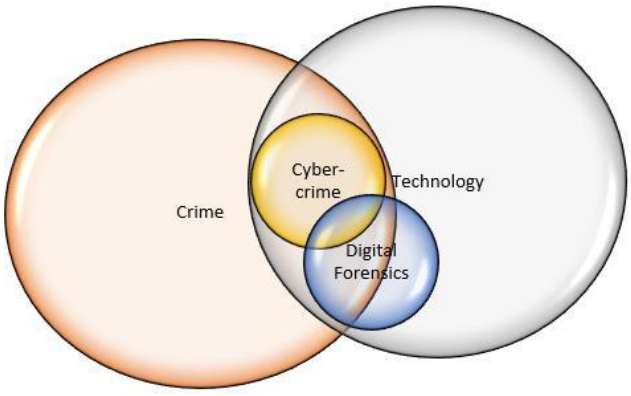

Fig. 1 - Relationship between cyber-crime and digital forensics (Arpitaet al, 2023)

Digital Forensics Models

A digital forensics model is a step-by-step procedure used for digital forensics investigation. Just like any other model, a digital forensic model depicts the sequence of investigation from beginning to end. According to Sigh and Guad, a digital forensics model is capable of providing an investigator with relevant information required during an investigation process (Singh & Gaud, 2015). The outcome of an investigation process is arguably a direct

product of the model used for the investigation. Several digital forensics models exist in digital forensic industries around the world, most of which are developed largely to suite already existing laws. This section will review different digital forensics models and comparing them side by side of the Nigerian investigation process. The first description of the use of digital forensics to investigate and prosecute crimes committed with the assistance of a computer or digital device was by Donn Parker's 1976 book, titled "Crime by Computer" (Kent & Karen, 2010). Digital Forensics deals with the investigation of crimes that involves digital devices, where a digital device contains evidence or information that can be useful in the prosecution of crime. Digital forensics is also referred to as computer forensics in some cases and may include subdivisions such as network forensics, Email forensics, and mobile forensics. It can be defined as the process of identification, acquisition, preservation, analysis, and documentation of any digital evidence (Lokhande & Meshram, 2015). Like almost every scientific endeavor, digital forensic started somewhere between an art and a craft (Chow & Shenoi, 2010). People with special skills and knowledge leveraged their skill sets and knowledge to put forth notions about the meaning of digital forensic in the context of legal matters. While the court system greatly appreciates science and its role through expert testimony in providing probative information, the appreciation is substantially challenged by the lack of a scientific base.

The Enhanced digital investigation process model

Florence, Venansius & Baryamruba (2004) identified the problem with the integrated digital investigation process model, hence they proposed a model that will separate investigation into primary(the computer),and secondary(the physical crime scene).The phases of this model are: Readiness, Deployment, Trace back, Dynamite, and Review. This model added two phases: the trace back, and dynamite as shown in figure 5.

Trace back is the 3rd phase of this model. It deals with the perpetrator's physical crime scene. It has two sub-phases namely: digital crime scene investigator, and authorization phase. Dynamite is the 4th phase of this model. It investigates the primary crime scene (the computer). At these phase items found in the computer are collected and analyzed. It has 4 sub-phases: physical crime scene, digital crime scene, reconstruction, and communication. This model in a bid to separate the investigations at the primary (computer), and the secondary (physical crime scene) made investigation complex for investigators trying to find their feet in digital forensics

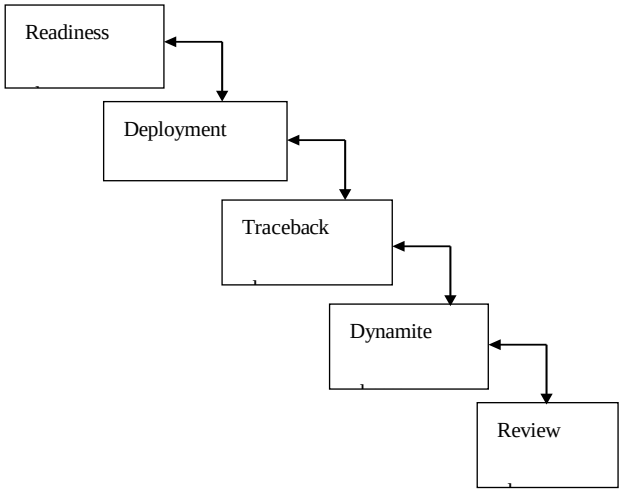

Figure 2:Phases of EIDIP Model (Source: Florence, Venansius & Baryamruba,2004)

Computer forensics field triage process model

Some cases are time-sensitive, Roger et al. (Roger, 2006) identified the importance of time in investigating cases such as kidnapping, Robbery, Terrorism, etc. He argued that the traditional models present at that time are not sufficient for acquiring clues from digital devices on the go to enable the apprehension of criminals before they flee to another country. This model is an Onsite model with 6 phases, namely: planning, triage, usage/user profile, Chronology/timeline, internet activity, and case-specific evidence (Roger, 2006). The phases of this model are derived partly from the Integrated Digital Investigation Process model (Brian et al., 2003) and partly from the Digital Crime Scene Analysis model (Marcus et al., 2006). Figure 6 shows the phases of this model.

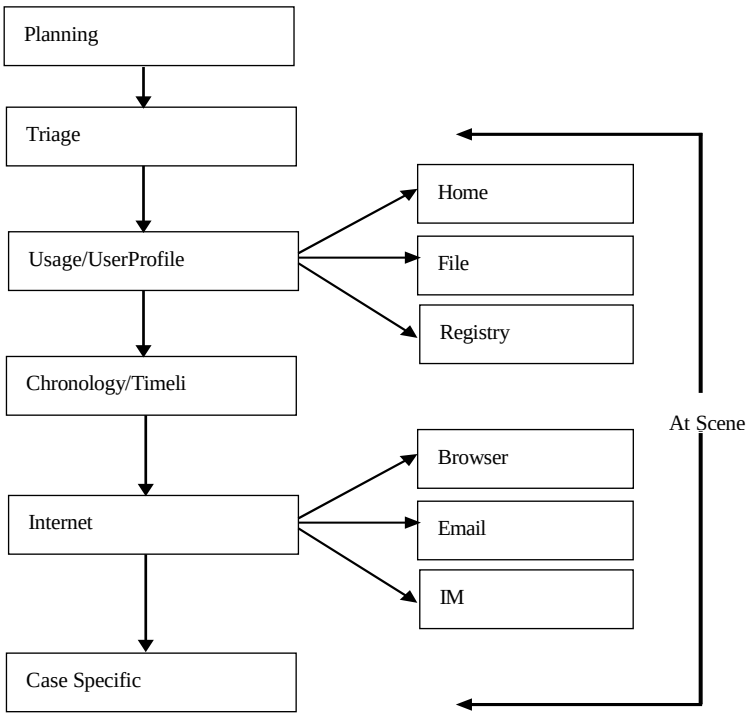

Figure 3: Phases of Computer Forensics Field Triage Process Model (Source: Rogeretal. (Roger, 2006)

Forensic Investigation of Small-Scale Digital devices

With technological advancements resulting in a more compact hand-held device with respect to size yet offering more storage on the hard drive and memory, the Internet of Things (IoT) realm condenses to comprise a subset of Small-Scale Digital Devices (SSDDs) that are nearly fit-in-your-pocket. Personal Data Assistants (PDAs) such as smartphones, tablets, and smart wearables, along with smart toys, gaming consoles, digital cameras, and drones are some of the more common SSDDs (Farkhund et al., 2023). There are applications of IoT devices and SSDDs in everyday life including wearable technology, fitness, smart homes, health care, smart cities, agriculture, industrial automation, etc. that emphasize their impact. Nearly every member of society uses a variety of IoT/SSDDs in today's digital world. Worryingly, with these devices, practically anything can be connected to the Internet or another "thing"– which highlights the fact that in many instances, we are creating our problems with a wider attack surface and underlying security issues (MacDermott, 2019). The accessibility of technology makes it easier for cybercriminals to utilize IoTs and SSDDs to covertly commit criminal activity. The Mirai malware targeted vulnerable IoT devices, such as those with default passwords and unsafe protocols turning them into a network of infected devices (also known as a botnet) that was used to flood targeted services with traffic, making them unavailable to normal users (Buxton, 2022). Fig. 2. 9 SSDDs such as smartphones, for example, store a lot of user data including calls, texts, images, and address books that may be subject to similar criminal activities (Nelson et al. 2014). Users' personal information is constantly at risk of threats and security lapses in the digital environment.

The usage of cyberspace for conducting criminal activity has introduced Digital Forensic (DF) investigation as a mandatory part of conventional investigations. For SSDD Forensics (SSDDF), past events are reconstructed to extract potential evidence from the device. This process encompasses various forensic analysis categories, i.e., (1) the type of Operating System (OS), (2) memory, (3) network, (4) browser, and (5) any paired device's investigation. Each branch of forensic analysis facilitates investigators to identify criminal activity performed in cyberspace in a holistic manner, which helps piece together information (artifacts) to establish the full picture (Maria Jones and Godfrey Winster, 2018).

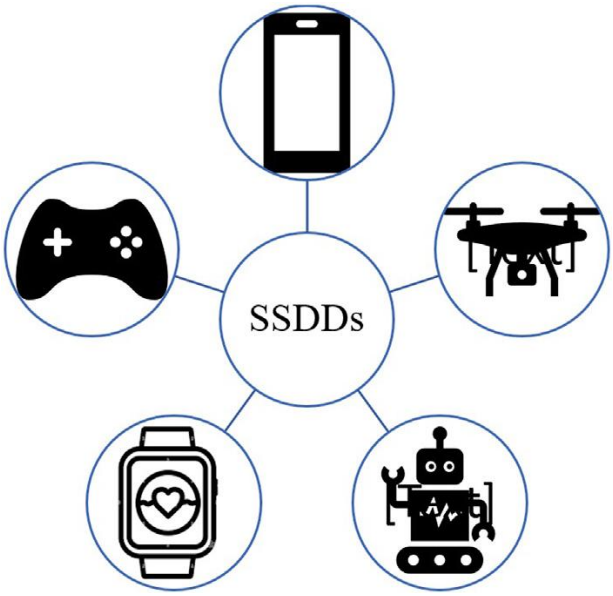

Figure 4:. Small Scale Digital Device. (Farkhund et al. 2023)

Useful artifacts concerning memory, OS, geo-location network activity, call logs, pictures, and videos can be extracted from IoT devices and SSDDs. In addition, browser history may store potential evidence. Memory artifacts, from slack and unallocated spaces, which preserve crucial information about running processes, are also the primary source of forensic artifacts. Digital devices are connected to the Internet by various means of communication, i.e., the wired network, Wi-Fi, Bluetooth Zigbee, ports, etc., and artifacts of forensic interest may be extracted from them.

The forensic processes in question pose challenges of various degrees. For example, finding the appropriate tool for forensic investigation is one of the major challenges because of diverse SSDDs. Such multifaceted issues stem from several variables such as different OSs, device models, and implemented security mechanisms that are constantly changing and evolving. In addition, jurisdictional issues present a unique barrier to forensic testing; only applicable laws are admissible in court. The entailing discussion elaborates on various other challenges in SSDD forensics and the use of cutting-edge technologies that may be utilized to annihilate them.

Table 1: Forensic frameworks comparison (Farkhund et al. 2023)

Research paper	Framework
Holistic digital forensic readiness framework for IoT-enabled organizations (Kebande et al., 2020)	An IoT framework based on ISO/IEC 27043; the authors adopt a holistic approach to cover the challenge of heterogeneity of various types of forensic artifacts extractable from an array of sources in an organizational structure; also performing a qualitative analysis of their framework.
Watch your smart watch (Al-Sharrah et al., 2018)	A framework for conducting smart watch forensics based on the physical backup, and wireless Communication stages of examination.
Forensic analysis of the nintendo 3ds nand (Pessolano et al. 2019)	A technique to extract and decode the data from the 3DS's NAND memory chip.
IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things (Zulkipli et al. 2017)	Various approaches comply with the inherent IoT characteristics; emphasizing the pre-investigation stage and using live investigation to make sure data and potential evidence are gathered and preserved throughout the investigation.

An Extended Model of Cybercrime Investigations

This is proposed. The phases or activities of the model are: awareness; authorization; planning; notification; search for and identify evidence; collection; transportation; storage; examination; hypothesis; presentation; proof/defences, and dissemination (Ciardhuáin, 2022). This may be considered as the more comprehensive model at that time. Table 2 shows different digital forensics tools or packages that are frequently employed in forensic investigations with their explanation and use (Tabona, 2018).

Table 2: Some Famous Digital Forensic Investigation Tools or programs (Ciardhuáin, 2022)

Tool	**Explanation**	**Use**
osquery	osquery is a constant monitor of the system state and does not target the restoration of deleted files.	Can detect Retefe Banking Trojan by continuous monitoring
FTK Imager	FTK Imager is a data preview and imaging tool that allows to examine files and folders on hard drives, network drives, CDs/DVDs, and review the content of forensic images or	SHA1 or MD5 hashes of files can be created. Then export files and folders from forensic images to disk. You can also view

	memories.	files in Windows Explorer
Last Activity View	Allow to view what actions were taken by a user and what events occurred on the machine Activities like running an executable file, opening a file/folder, an application or system crash or a user performing a software installation will be registered in a log file.	The information can be exported to a CSV / XML HTML file. This tool is useful when you need to prove that a user performed an action he denied.
GRR	The main benefit of GRR is its capability to check actual file content and search for strings that can be attributed to known malware It allows looking for changed files in the overall OS structure.	GRR Rapid Response is an incident response framework focused on remote live forensics.GRR consists of two parts: client and server. It works just like osquery
Paladin Forensic Suite	Paladin Forensic Suite is a Live CD based on Ubuntu that is packed with many open source forensic tools.	There are over 80 tools on this CD dealing with Imaging, Malware Analysis, Social Media Analysis, Hashing, etc.
USB Historian	It parses USB information, from the Windows registry, to give a list of all USB drives that were plugged into the machine. It displays information such as the name of the USB drive, the serial number, when it was mounted and by which user.	These information can be very useful when you need to understand whether the data was removed, moved, or accessed
Autopsy (Sleuth Kit)	It is a digital forensics platform with a GUI that is used to understand what happened on a computer.	It comes with features like; Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching It can recover deleted files from unallocated space.
CAINE (Computer Aided Investigative Environment)	It is a Linux Live CD. Features include a GUI, semi automated report creation and tools for Mobile Forensics, Network Forensics, and Data Recovery	CAINE environment is designed to assist investigators in all four stages of an investigation: preservation, collection, examination, and analysis
COFEE (Computer Online Forensic Evidence Extractor)	It MS toolkit acts as an automated forensic tool during a live analysis. It contains features and a GUI that guides you through data collection and examination and helps generate reports after extraction..	It is a forensic toolkit used to extract evidence from MS Windows computers
Wireshark	It is used by governments and big corporate across the world. It enables looking at a network at the microscopic level. then admin can scan for malicious activity.	It is the world's most-used network protocol analysis tool. It may be used with Xplico tool. You can extract e-mails.

The Liforac Model (Bobber, 2009) is a live forensic acquisition processing model that collects the evidence from live acquisition to counter the problems caused by dead acquisitions them into a legally framework. The developed model followed basic concept of Liforac Model but unlike the Liforac Model's technical key pillars they adopted key principles Reconnaissance, Relevancy and Reliability but the working sense is similar. The model also paid full attention on flow of process according with the judiciary norms which also been done in Liforac Model (Bobber, 2009) The Hybrid Model of Magkos (Vlachopoulo, 2022)adopted the same guidelines that mentioned in the two previous models that concentrated on filling the gap in-between physical and digital evidence. Their research used the chain of custody platform to develop their model; their work presented a basic concept of chain of custody of digital evidence" and "life cycle of digital evidence". It addressed an additional phase in the life cycle in digital archiving. Again like the previous models this model has limitation in other phases.

Methodology :

The research adopted a triangulation research methodology. This research methodology combines qualitative and quantitative research methodologies. Survey and interview was conducted to investigate the effectiveness of crime investigation types used in Nigeria with a view to understanding their effects on criminal investigations and recommending a type that may improve crime investigation among law enforcement agencies. The population of the study comprised of a stratified sampling of 184 participants from security agents from Economic and Financial Crimes Commission (EFCC), Department of Security Services (SSS), Independent Corrupt Practices Commission (ICPC), Nigeria Police Force (NPF), Nigeria Immigration Services (NIS), and Nigeria Drug Law Enforcement Agency (NDLEA). The sample size was calculated using the Taro-Yamane formula and the sample size was calculated to be 184.

Table 3: Population of the Study

Name of security agency	Number of investigators
EFCC	50

DSS	60
ICPC	40
NPF	100
NIS	70
NDLEA	20
TOTAL	**340**

Source: Researcher's Field Work, 2022

Therefore

$$n = \frac{340}{1 + 340(0.05)^2}$$

n = 183.7

$$n \cong \frac{340}{1 + 340(0.0025)}$$

n 184

$$n = \frac{340}{1.85}$$

Therefore, sample size for the study is 184forPre-design quantitative study.

The calculated sample size proportion is presented in a tabular form in Table 2.

Table 3: Population and sample size proportion of the study drawn from the six security agencies.

S/N	Security agencies	Population	Sample Size Proportion
	EFCC	50	27
	SSS	60	32
	ICPC	40	22
	NPF	100	54
	NIS	70	38
	NDLEA	20	11
	TOTAL	**340**	**184**

Architecture of the Proposed System :

Figure 5, describes the proposed the architecture of the proposed system, the proposed enables data to store in real time. It contain a web API/database that data crime log and responses.

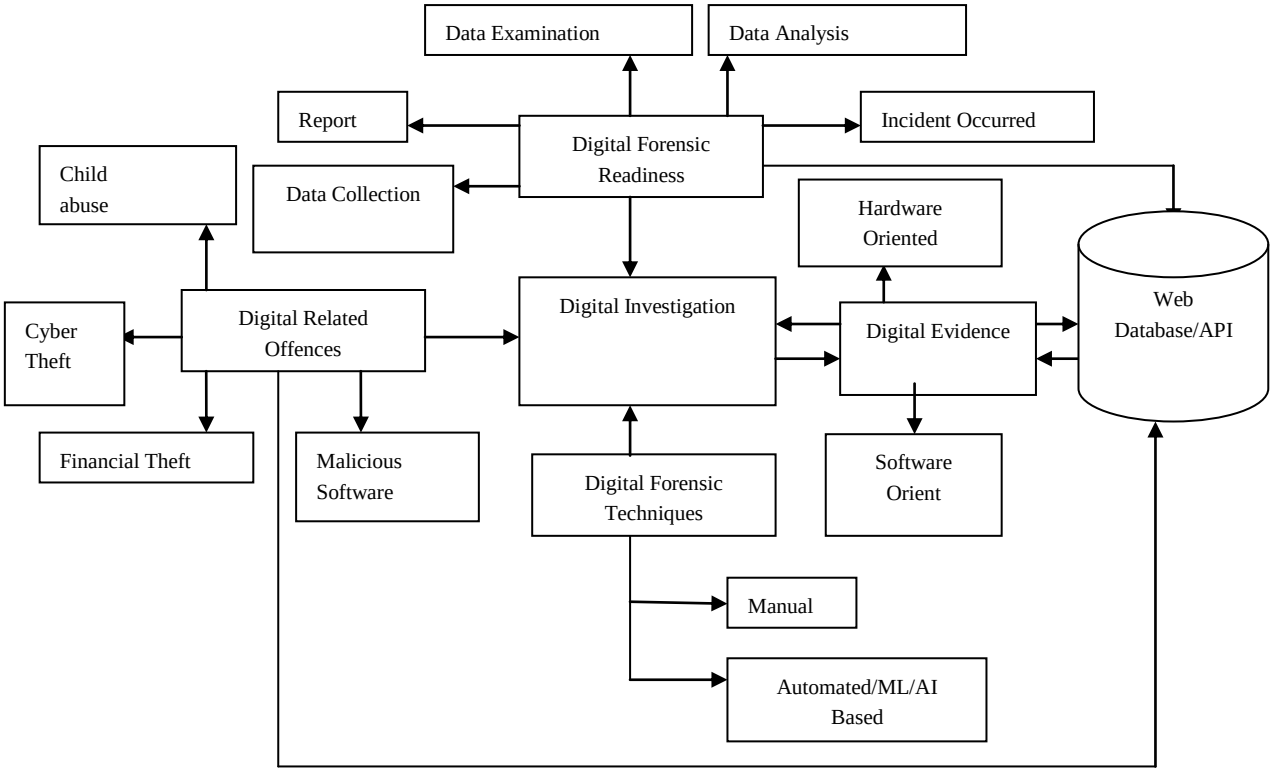

Figure 5: Architecture of the Proposed System

CODES FOR DEFINING THE DATABASE TABLES AND THEIR ATTRIBUTES :

```
from django.db import models
from accounts.models import Investigator
select_category = (
    ('TAR', 'Theft and Robbery'),
    ('B', 'Burglary'),
    ('PR', 'Offence against Property'),
    ('SO', 'Sexual offence'),
    ('MVO', 'Motor vehicle offence'),
    ('FD', 'Forced disappearance'),
    ('P', 'Piracy'),
    ('SS', 'Sexual slavery'),
    ('CL', 'Child labour'),
    ('DRC', 'Drug related case'),
    ('K', 'Kidnapping'),
    ('FI', 'False Imprisonment'),
    ('MC', 'Murder Case'),
    ('O', 'other'),
   ('ASA', 'Assault and Battery'),
   ('VND', 'Vandalism'),
   ('FRD', 'Fraud'),
   ('DNM', 'Drug Manufacturing'),
   ('DV', 'Domestic Violence'),
```

```
    ('ARS', 'Arson'),
    ('HRS', 'Homicide'),
    ('ECP', 'Embezzlement'),
    ('HSM', 'Harassment'),
    ('DUI', 'Driving Under the Influence'),
    ('SCX', 'Sexual Coercion'),
    ('CYP', 'Cyberbullying'),
    ('WFS', 'Weapons Offense'),
    ('HBT', 'Human Trafficking'),
)
report_status = (
    ('VALID', 'VALID'),
    ('ACTIVE', 'ACTIVE'),
    ('DISMISSED', 'DISMISSED')
)
class Report(models.Model):
    title = models.CharField(max_length=500)
    photo = models.ImageField(null=True, blank=True)
    category = models.CharField(max_length=3, choices=select_category)
    description = models.TextField()
    reporter = models.CharField(max_length=200)
    incident_date = models.DateField()
    incident_time = models.TimeField()
    approved = models.BooleanField(default=False)
    timestamp = models.DateTimeField(auto_now_add=True)
    updated = models.DateTimeField(auto_now=True)
    status = models.CharField(max_length=10, choices=report_status, default='VALID')
    def __str__(self):
        return f"{self.incident_date} - {self.title}"


class Case(models.Model):
    number = models.CharField(max_length=50, null=True, blank=True)
    report = models.ForeignKey(Report, on_delete=models.CASCADE)
    investigator = models.ForeignKey(Investigator, on_delete=models.CASCADE )
    authorization_letter = models.ImageField(null=True, blank=True)
    time_opened = models.DateTimeField(auto_now_add=True)
    time_closed = models.DateTimeField(null=True, blank=True)
    updated = models.DateTimeField(auto_now=True)
    isdismissed = models.BooleanField(default=False, blank=True, null=True)
    isresolved = models.BooleanField(default=False, blank=True, null=True)

    def get_case_number(self):
        return f"CS/{self.id}I{self.investigator.id}/RP/{self.report.id}"
    def save(self, *args, **kwargs):
        self.number = self.get_case_number()
        super().save(*args, **kwargs)
    def __str__(self):
        if self.time_closed:
            closed_date = f"to {self.time_closed}"
        else:
            closed_date = ''
        return f"{self.investigator.name} | {self.number} | {self.time_opened} {closed_date}"

class Investigator(models.Model):
    user = models.ForeignKey(User, on_delete=models.CASCADE)
    name = models.CharField(max_length=200)
    logo = models.ImageField(null=True, blank=True, default='static/images/evidence.jpg')
    address = models.CharField(max_length=200)
    phone = models.CharField(max_length=15)
```

```
    email = models.EmailField()
    specializations = models.ManyToManyField('Specialization', blank=True)

    def __str__(self):
        return self.name

class Specialization(models.Model):
    name = models.CharField(max_length=3, choices=select_category, unique=True)

    def __str__(self):
        return self.get_name_display()

class Timeline(models.Model):
    date=models.DateField(auto_now_add=True)
    description = models.TextField()
    case = models.ForeignKey(Case, null=False, blank=False, on_delete=models.CASCADE)
    def __str__(self):
        return f"{self.case.number} - {self.description}"
class Evidence(models.Model):
    serial_no = models.CharField(max_length=20, null=True, blank=True)
    case = models.ForeignKey(Case, on_delete=models.CASCADE, related_name='evidences', null=True, blank=True)
    title = models.CharField(max_length=100)
    scene_description = models.TextField()
    photo = models.ImageField( null=True, blank=True)
    acquisition_date = models.DateField()
    acquisition_time = models.TimeField()
    acquisition_by = models.CharField(max_length=200)
    acquisition_tools = models.CharField(max_length=255)
    packaging = models.CharField(max_length=255, null=True, blank=True)
    packaged_by = models.CharField(max_length=255, null=True, blank=True)
    transported_by = models.CharField(max_length=255, null=True, blank=True)
    examiner = models.CharField(max_length=255, null=True, blank=True)
    examination_tools = models.CharField(max_length=255, null=True, blank=True)
    examination_time = models.TimeField(null=True, blank=True)
    examination_date = models.DateField(null=True, blank=True)
    evidence_analysis = models.TextField(null=True, blank=True)
    def __str__(self):
        return f"{self.serial_no} - Evidence of: {self.title}"
    def get_serial_no(self):
        return f"EV/{self.id}/{self.case.number}"
    def save(self, *args, **kwargs):
        super().save(*args, **kwargs)
        self.serial_no = self.get_serial_no()
        super().save(*args, **kwargs)
```

CODES FOR THE VARIOUS ROUTING VIEWS

```
 from django.contrib.auth import authenticate, login
from django.shortcuts import render, redirect, HttpResponse
from django.contrib import messages
from django.contrib.auth import logout
from django.urls import reverse
from django.contrib.auth.decorators import login_required

from .forms import ReportForm, CaseForm
from .models import Report, Evidence, Timeline
from .models import Case as CaseModel
from accounts.models import Investigator
from django import forms
from django.db.models import Case, When, Value, IntegerField, Q
from .decorators import investigator_case_required
```

```
################
#   AUTHENTICATION RELATED VIEWS
################

def login_view(request):
    if request.method == 'POST':
        username = request.POST.get('username')
        password = request.POST.get('password')
        user = authenticate(request, username=username, password=password)
        if user is not None:
            login(request, user)
            #return HttpResponse("You are successfully logged in")
            return redirect('dashboard')
        else:
            # Return an error message if authentication fails
            messages.error(request, 'Invalid username or password.')
            return HttpResponse("Wrong Details")
    return render(request, 'login.html')  # Render the login form template

def logout_view(request):
    logout(request)
    return redirect(reverse('login'))
```

Sample Output

Fig. 6-12 show the sample output for the web application for reporting crimes within security agencies

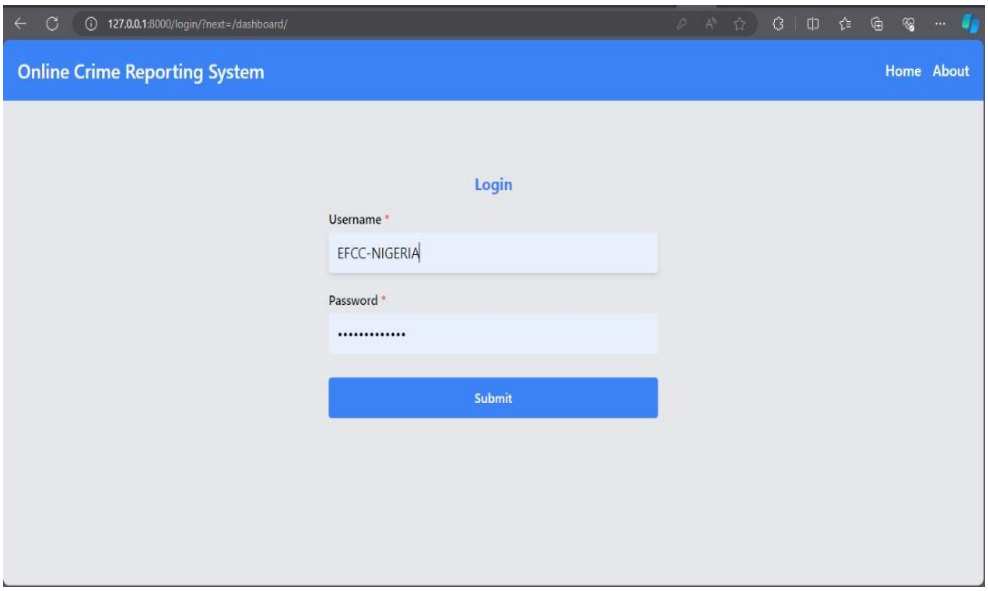

Figure 6: NPF Authentication and Authorization

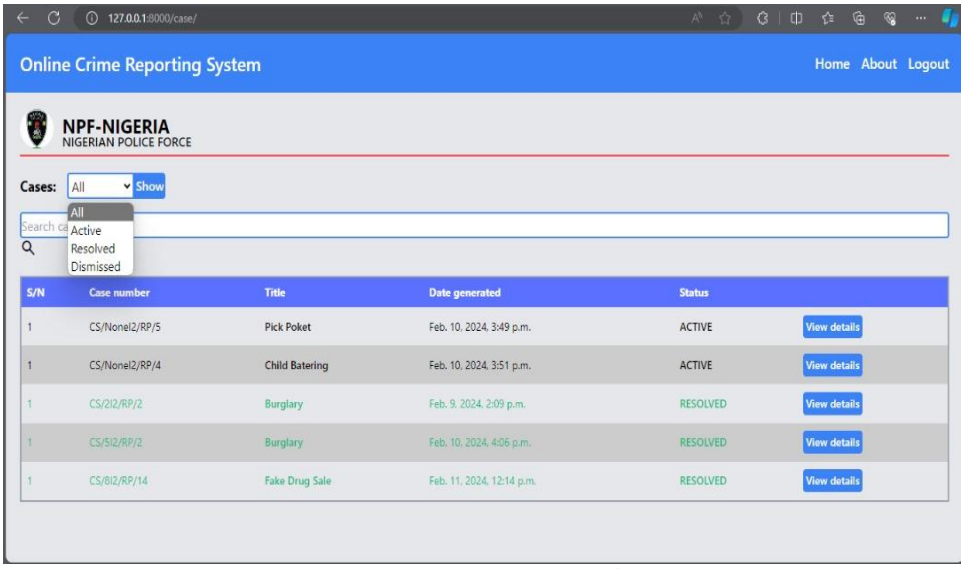

Figure 7: NPF Nigeria view details of report

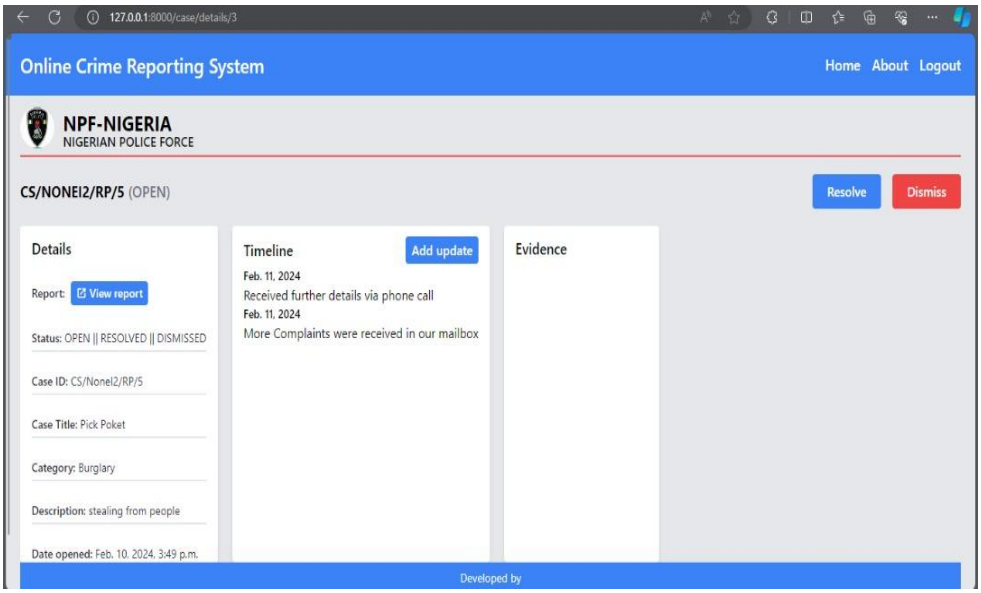

Figure 8: NPF View details

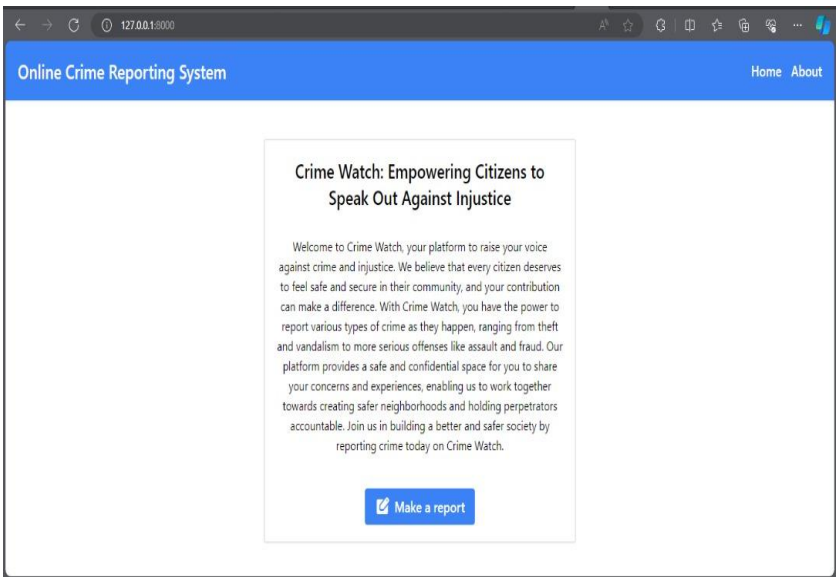

Figure 9: NPF Report Page

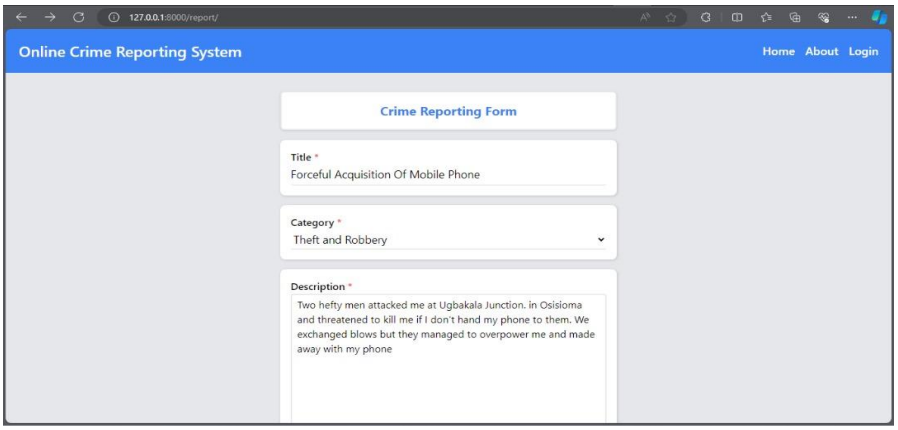

Figure 10: Crime Reporting Form

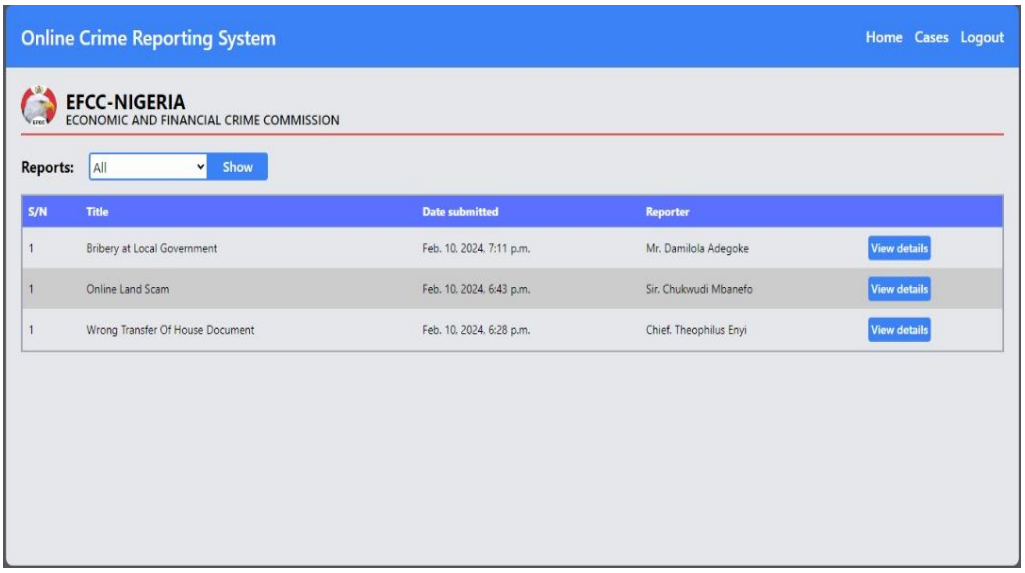

Figure 11: EFCC Back-end page

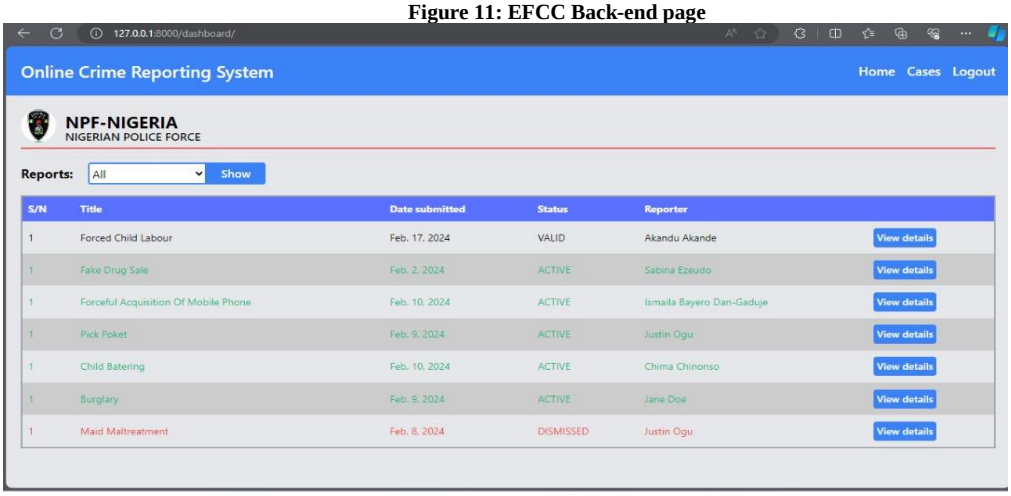

Figure 12: Crime Reporting Form

This work has demonstrated and developed an application for digital tracking and investigation of crime for security agencies. A robust enables crime reporting systems that create independent jurisdictions for enforcement of crime.

CODES FOR DEFINING THE DATABASE TABLES AND THEIR ATTRIBUTES

```
from django.db import models
from accounts.models import Investigator
select_category = (
    ('TAR', 'Theft and Robbery'),
    ('B', 'Burglary'),
    ('PR', 'Offence against Property'),
    ('SO', 'Sexual offence'),
    ('MVO', 'Motor vehicle offence'),
    ('FD', 'Forced disappearance'),
    ('P', 'Piracy'),
    ('SS', 'Sexual slavery'),
    ('CL', 'Child labour'),
    ('DRC', 'Drug related case'),
    ('K', 'Kidnapping'),
    ('FI', 'False Imprisonment'),
    ('MC', 'Murder Case'),
    ('O', 'other'),
   ('ASA', 'Assault and Battery'),
   ('VND', 'Vandalism'),
   ('FRD', 'Fraud'),
   ('DNM', 'Drug Manufacturing'),
   ('DV', 'Domestic Violence'),
   ('ARS', 'Arson'),
   ('HRS', 'Homicide'),
   ('ECP', 'Embezzlement'),
   ('HSM', 'Harassment'),
   ('DUI', 'Driving Under the Influence'),
   ('SCX', 'Sexual Coercion'),
   ('CYP', 'Cyberbullying'),
   ('WFS', 'Weapons Offense'),
   ('HBT', 'Human Trafficking'),
)
report_status = (
   ('VALID', 'VALID'),
   ('ACTIVE', 'ACTIVE'),
   ('DISMISSED', 'DISMISSED')
)
class Report(models.Model):
   title = models.CharField(max_length=500)
   photo = models.ImageField(null=True, blank=True)
   category = models.CharField(max_length=3, choices=select_category)
   description = models.TextField()
   reporter = models.CharField(max_length=200)
   incident_date = models.DateField()
   incident_time = models.TimeField()
   approved = models.BooleanField(default=False)
   timestamp = models.DateTimeField(auto_now_add=True)
   updated = models.DateTimeField(auto_now=True)
   status = models.CharField(max_length=10, choices=report_status, default='VALID')
   def __str__(self):
      return f"{self.incident_date} - {self.title}"


class Case(models.Model):
   number = models.CharField(max_length=50, null=True, blank=True)
   report = models.ForeignKey(Report, on_delete=models.CASCADE)
   investigator = models.ForeignKey(Investigator, on_delete=models.CASCADE )
   authorization_letter = models.ImageField(null=True, blank=True)
```

```
    time_opened = models.DateTimeField(auto_now_add=True)
    time_closed = models.DateTimeField(null=True, blank=True)
    updated = models.DateTimeField(auto_now=True)
    isdismissed = models.BooleanField(default=False, blank=True, null=True)
    isresolved = models.BooleanField(default=False, blank=True, null=True)

    def get_case_number(self):
        return f"CS/{self.id}I{self.investigator.id}/RP/{self.report.id}"
    def save(self, *args, **kwargs):
        self.number = self.get_case_number()
        super().save(*args, **kwargs)
    def __str__(self):
        if self.time_closed:
            closed_date = f"to {self.time_closed}"
        else:
            closed_date = ''
        return f"{self.investigator.name} | {self.number} | {self.time_opened} {closed_date}"

class Investigator(models.Model):
    user = models.ForeignKey(User, on_delete=models.CASCADE)
    name = models.CharField(max_length=200)
    logo = models.ImageField(null=True, blank=True, default='static/images/evidence.jpg')
    address = models.CharField(max_length=200)
    phone = models.CharField(max_length=15)
    email = models.EmailField()
    specializations = models.ManyToManyField('Specialization', blank=True)

    def __str__(self):
        return self.name

class Specialization(models.Model):
    name = models.CharField(max_length=3, choices=select_category, unique=True)
    def __str__(self):
        return self.get_name_display()
class Timeline(models.Model):
    date=models.DateField(auto_now_add=True)
    description = models.TextField()
    case = models.ForeignKey(Case, null=False, blank=False, on_delete=models.CASCADE)
    def __str__(self):
        return f"{self.case.number} - {self.description}"
class Evidence(models.Model):
    serial_no = models.CharField(max_length=20, null=True, blank=True)
    case = models.ForeignKey(Case, on_delete=models.CASCADE, related_name='evidences', null=True, blank=True)
    title = models.CharField(max_length=100)
    scene_description = models.TextField()
    photo = models.ImageField( null=True, blank=True)
    acquisition_date = models.DateField()
    acquisition_time = models.TimeField()
    acquisition_by = models.CharField(max_length=200)
    acquisition_tools = models.CharField(max_length=255)
    packaging = models.CharField(max_length=255, null=True, blank=True)
    packaged_by = models.CharField(max_length=255, null=True, blank=True)
    transported_by = models.CharField(max_length=255, null=True, blank=True)
    examiner = models.CharField(max_length=255, null=True, blank=True)
    examination_tools = models.CharField(max_length=255, null=True, blank=True)
    examination_time = models.TimeField(null=True, blank=True)
    examination_date = models.DateField(null=True, blank=True)
    evidence_analysis = models.TextField(null=True, blank=True)
    def __str__(self):
        return f"{self.serial_no} - Evidence of: {self.title}"
```

```
    def get_serial_no(self):
        return f"EV/{self.id}/{self.case.number}"
    def save(self, *args, **kwargs):
        super().save(*args, **kwargs)
        self.serial_no = self.get_serial_no()
        super().save(*args, **kwargs)
```

CODES FOR THE VARIOUS ROUTING VIEWS

```
 from django.contrib.auth import authenticate, login
from django.shortcuts import render, redirect, HttpResponse
from django.contrib import messages
from django.contrib.auth import logout
from django.urls import reverse
from django.contrib.auth.decorators import login_required

from .forms import ReportForm, CaseForm
from .models import Report, Evidence, Timeline
from .models import Case as CaseModel
from accounts.models import Investigator
from django import forms
from django.db.models import Case, When, Value, IntegerField, Q
from .decorators import investigator_case_required
################
#   AUTHENTICATION RELATED VIEWS
###############
def login_view(request):
    if request.method == 'POST':
        username = request.POST.get('username')
        password = request.POST.get('password')
        user = authenticate(request, username=username, password=password)
        if user is not None:
            login(request, user)
            #return HttpResponse("You are successfully logged in")
            return redirect('dashboard')
        else:
            # Return an error message if authentication fails
            messages.error(request, 'Invalid username or password.')
            return HttpResponse("Wrong Details")
    return render(request, 'login.html')  # Render the login form template

def logout_view(request):
    logout(request)
    return redirect(reverse('login'))
```

Conclusion :

The understanding of the problems that are very peculiar to criminal investigation in Nigeria was opened up in this work. The research shows that the inconsistent judgments and discharge and acquittal of cases in Nigeria are as a result of a lack of a standardized digital forensics model. Unfortunately, different security and law enforcement agencies in Nigeria have different standard operating procedures for criminal investigations as shown by this research work. Hence one cannot categorically say that Nigeria has a standardized digital forensics model for use by the security and law enforcement agencies. The lack of a generally acceptable digital forensics model poses great challenges for criminal investigations and prosecution in Nigeria. The admissibility of digital evidence is based on the steps (digital forensics model) used for the collection of such evidence. If the correct steps are not followed when collecting evidence, such evidence will not be admissible. Another challenge is the time spent in investigating a crime. With a digital forensics model, an investigator can save time and resources, since the model guides an investigator on what to do and how to do it. To reiterate, the lack of a digital forensic model has resulted in conflicting results from digital forensics examinations by forensics units and experts within the Nigerian Law Enforcement community. The introduction of a digital forensics model implemented in the software will to a large extent reduce the crime rate in Nigeria. Hence a digital forensics model is required for the effective investigation and prosecution of crimes in Nigeria. The lack of effective and efficient application of digital forensics in criminal investigations in Nigeria is arguably attributable to the lack of standardized processes and procedures (digital forensic model) for adoption by various law enforcement agents in Nigeria and the absence of a regulatory body. This has

consequently affected criminal hearings, where different security and law enforcement agents apply different SOP which results in the presentation of conflicting forensic expert reports. In conclusion, the adoption of this newly designed Enhanced Forensics Process Model implemented in the software will enhance the practice of digital forensics in Nigeria.

REFERENCES :

1. ACT (2015) Administration of Criminal Justice Act 8 February, 2016 retrieved from **http://www.lawpavilion.com/blog/administration-of-criminal-justice-act-2015-acja/Accessed** 16/6/2020 [16:20:34]
2. Agarwal, A .,& Gupta, M.(2011).Systematic Digital Forensic Investigation Model.
3. *International Journal of Computer Science and Security (IJCSS),Volume(5):Issue(1)*, 118 -131.
4. Arpita S. Singh, S. K. Nilu S. and Sandeep K. N. (2023) An Algorithm for Crime Detection in Digital Forensics Journal of Survey in Fisheries Sciences 10(3S) 1281-1290 2023
5. Al-Khateeb, Haider, Gregory Epiphaniou, Herbert Daly. Blockchain for modern digital forensics: the chain-of-custody as a distributed ledger Blockchain and Clinical Trial: Securing Patient Data. 2019: 149-68.
6. Ariffin KAZ, Ahmad FH. Indicators for maturity and readiness for digital forensic investigation in era of Industrial Revolution 4.0. Comput Sec. 2021; 105: 102237.
7. Ajumoke,N.(2018)buzznigeria.Retrievedfromhttps://buzznigeria.com/top-20-online-shopping stores-in-Nigeria/ Accessed 16/6/2020.
8. Allen,J.(2015) Information Systems ,Dominant Paradigms, and Engineering Concepts: A Community Clustering Analysis of the Highest Impact Topics in Information Systems Research. Entrepreneurship, Innovation, and Strategy. Page 22 retrieved from http://repository.usfca.edu/esib/22
9. Applegate, L.M.(1999).Rigosr and Relevance in Management Information System Research- Introduction. Quarterly, 23(1), 1-2.
10. Anwaar Iftikhar*; Rida Farooq; Mehvish Mumtaz; Sana Hussain; Mubeen Akhtar; Muhammad Ali; Ghulam Zahara Jahngir (2023) Quality Assurance in Digital Forensic Investigations: Optimal Strategies and Emerging Innovations, Austin Journal of Forensic Science and Criminology, . Austin J Forensic Sci Criminol. 2023; 10(2): 1097
11. Alhaboby ZA, Al-Khateeb HM, Barnes J, Short E. The language is disgusting and they refer to Short E. my disability: the cyberharassment of disabled people. Disabil Soc. 2016; 31: 1138-43. 20.
12. Alhaboby ZA, Alhaboby D, Al-Khateeb HM, Epiphaniou G, Ismail DKB, Jahankhani (2018) Understanding the cyber-victimisation of people with long term conditions and the need for collaborative forensics-enabled disease management programmes. In: Jahankhani H, editor. Cyber criminology. Advanced sciences and technologies for security applications. Cham: Springer. 2018; 227-50.
13. Bulbul HI, Yavuzcan HG, Ozel M. Digital forensics: an analytical crime scene procedure model (ACSPM). Forensic Sci Int. 2013; 233: 244-56.
14. Bobbler.M.M, Solms S.H.von (2009). Modelling Live Forensic Acquisition, Workshop on digital Forensic Incident analysis (WDFIA)
15. Bhat WA, AlZahrani A, Wani MA (2021). Can computer forensic tools be trusted in digital investigations? Sci Justice. 2021; 61: 198-203.
16. Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process Modelin: *Proceedings of the Fourth Digital Forensic Research Workshop*,pp.1-9.
17. Brian, C. & Eugine, H .Spafford (2003) getting physical with the Investigation Process.
18. *International journal of digital evidence*. Fall 2003,volume 2 ,issue2.
19. Carlton, G.H.(2007).A grounded theory approach to identifying and measuring forensic data acquisition tasks. *Journal of Digital Forensics, Security and Law*, 2(1), 35-55.
20. Carrier, B.D.(2006).A hypothesis-based approach to digital forensic investigations .Pro Quest
21. pp.8(6),88-94.
22. Ciardhuáin, SO (2022).: An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2022.
23. Chijiok, C.E.(2013)Crime and Criminal Investigation in Nigeria: A Study of Police Criminal Investigation in Enugu State: International Journal of African and Asian Studies – An *Open Access International Journal* Vol.1 2013, pp. 66-72
24. Chow, K.P., & Shenoi, S.(2010).Toward a science of digital forensic evidence examination .
25. Advancesin Digital Forensics VI, IFIPAICT337, 17–35.
26. Cohen, F. (2008). Challenges to digital forensics evidence. Livermore, CA: ASP Press.pp. 47-86
27. Cohen, L., Manion, L. ,& Morrison,K.(2011).Research methods in education.Routledge.Vol.1 pp.66-72.
28. Copyright Act(2004) retrieved fromttp://www.mondaq.com/Nigeria/x/692416/An+Overview+Of+Copyright+Protection+In+Nigeria+Part+1/Accessed 12/6/2020
29. Creswell, J. W. (2008) Research Design: Qualitative, Quantitative, and Mixed Method Approaches. Thous and Oaks, Calif.: London: Sage Publications.Vol.12013,pp.66-72
30. Cunningham, A.(2018,January29).*News*. Retrieved from CBC News:
31. www.cbc.ca/amp/1.4507272Accessed 15/6/2020.
32. Dasuki (2014) National Cyber Security Policy. Retrieved from ttps://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf Accessed 11/6/2020
33. Dwan, C.(2018,January4).Notable Computer Forensics Cases .Retrieved from Infosec Institute :ttps:0//resources. infosec institute.com/category/computer forensics/ introduction/notable-computer-forensics-cases/#gref Accessed 12/4/2020.

34. Ebo, N. (2016, June 4). 10-major-crimes-committed-in-nigeria. Retrieved from Legal7676: https://legal7676.wordpress.com/2016/07/01/10-major-crimes-committed-in-nigeria Accessed 11/6/2020.
35. FBI. (2010). Property Crime. Retrieved from FBI's Uniform Crime Reporting: https://ucr.fbi.gov/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/property-crimeAccessed 11/6/2020.
36. FBI.(2016,August24).*ViolentCrime*.RetrievedfromUCI:(https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/violent-crime. 11/6/2020.
37. Frechtling J & Sharpe L(1997) User Friendly Handbook for Mixed Method Evaluations.
38. Retrieve from http://www.nsf.gov.pubs/1997/nsf97153. Accessed11/6/2020.
39. Frye V.(1923).Design Research in InformationSystems.NewYork:Springer.Vol.1pp.56-75.
40. Hall, B .& Howard, K.(2008)A Synergistic Approach :Conducting Mixed Methods Research With Typological and Systemic Design Considerations. Journal of Mixed Methods Research, 2(3) 248-269.
41. Horsman G. Digital evidence strategies for digital forensic science examinations. Sci Justice. 2023; 63: 116-26.
42. Henry Umoru (2017, May 24) $450m lost to cyber crime in Nigeria —Senate. Retrieve fromVangaurdNews:https://www.vanguardngr.com/2017/05/450m-lost-cyber-crime-nigeria-senate/
43. Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems .New York: Springer.Vol.1 pp. 56-75.
44. Horsman G. Tool testing and reliability issues in the field of digital forensics. Digit Investig. 2019; 28: 163-75.
45. Hill, K. (2011, November 3). *Tech*. Retrieved from Forbes:https://www.forbes.com/sites/kashmirhill/2011/11/03/solving-a-teen-murder-by-following-a-trail-of-digital evidence/#36bb03b61833
46. Horsman G. 'Scaffolding' responses to digital forensic inquiries. Wiley Interdiscip Rev Forensic Sci. 2022; 4: e1451.
47. Humphries G, Nordvik R, Manifavas H, Cobley P, Sorell M. Law Enforcement educational challenges for mobile forensics. Forensic science international. Digit Investig. 2021; 38: 301129.
48. Intelligence, B. (2017, july 6). Bulwark Intelligence. Retrieved from Bulwark Intelligence: http://bulwarkintelligence.com/reports/crime/best-way-solve-crime-bank-offer-moneyAccessed 13/5/2020.
49. Internet World Stats (2019) Usage and Population Statistics. Retrieved fromhttps://www.internetworl tats.com/. Accessed 12/6/2020
50. Janet, W. (2012). ACPO Good practice guide for digital evidence. Available at https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/.Accessed 12/5/2020.
51. Jannah, C. (2017,August22).Daily Post Nigeria News .Retrieved from Daily Post Nigeria: www.dailypost.ng/. Accessed 2017/8/22.
52. Johnson, R., Onwuegbuzie, A. & Turner,L.(2007) Toward a Definition of Mixed Methods
53. *Research. JournalofMixedMethodsResearch*,1(2)112-133.
54. Kent, & Karen.(2010).Guide to integrating forensic techniques in to incident response .NY: NIST Special Publication. Vol. 2 45-55. Accessed 11/5/2020
55. Kessler, G.C.(2010). Judges'awareness ,understanding ,and application of digital evidence Doctoral dissertation, Nova Southeastern University Vol. 1. Pp. 66-87 Accessed 11/5/2020.
56. Kohn, M., Eloff, J. ,& Olivier, M.(2010). Framework for a digital forensic investigation.
57. Information and Computer Security Architectures Research Group(ICSA).Vol.1pp.68- 99
58. Lokhande, P., & Meshram,B.(2015).Digital Forensics Analysis for Data Theft. *The International Journal of Forensic Computer Science*, Vol. 5 pp. 30-51.
59. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. Proceedings of the 11th Annual ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Daytona Beach, Florida, 24-26 May 2016, pp. 24-26. https://
60. Macionis, Gerber, John, &Linda.(2010). Practical Strategies for Combining Qualitative
61. *Sociology7thCanadianEd.* Toronto,Ontario:PearsonCanadaInc.pp.206.
62. Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge & Steve Debrota (2006).
63. Computer Forensics Field Triage Process Model. *Journal of Digital Forensics ,security and law*. Vol. 1 pp. 60-75
64. Michael K. (2015). Tech Republic. Retrieved from www.techrepublic.com/article/digital- forensics-resembles-the-wild-west-when-it-comes-to-regulation/Accessed20/4/2020
65. Miniwatts (2019) Internet World Stats. Retrieved fromhttps://www.internetworldstats.comAccessed 20/4/2020.
66. Morgan, D.(1998) Practical Strategies for Combining Qualitative and Quantitative
67. Methods: Application to Health Research .Qualitative Health Research,8(3)362-376.
68. Moffatt-Bruce SD, Ferdinand FD, Fann JI. Patient safety: disclosure of medical errors and risk mitigation. Ann Thorac Surg. 2016; 102: 358-62
69. National Information Technology Development agency [NITDA] (2014).Standards for digital and Computer Forensics in Nigeria. Draft vol.2. Retrieved from https://www.scribd.com/document/287428618/Guidelines-on-Digital-Forensic-pdf.
70. National Institute of Justice (NIJ)(2001)Electronic crimes scene investigation guide :guide for first responders .National Institute of Justice ,Department of Justice (DoJ)2001.Available at http://www.ncjrs.gov/pdffiles1/nij/187736.pdf.
71. Nielsen (2012) Social Media Report 2012 Retrieved from https://www.nielsen.com/us/en/insights/article/2012/social-media-report-2012-social- media-comes-of-age/
72. Nigeria: Evidence Act, 2011 [Nigeria], 3 June, 2011 available at http://www.refworld.org/docid/54f86b844.htmlAccessed20/4/2020
73. Nnochiri, I. (2017, June 7). Boko Haram Sponsorship. Retrieved from Vanguard News: https://www.vanguardngr.com/2017/06/boko-

haram-sponsorship-ndume-case-answer-fg-tells-court-2Accessed 21/5/2020

74. Noblis (2007) Metrics for the evaluation of regional law enforcement information shearing systems. Retrieved from https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.ncjrs.gov/pdffiles1/nij/grants/219377.pdf &ved=2ahUKEwjo5aep0P7xAhVeQUEAHWB5D9IQFjAAegQIAxAC&usg=AOvVaw0nhfqVEJKYGWrjISVBZ2PIAccessed 29/5/2020
75. Noel Out (2018).The Nigeria Police Forensic Investigation Failure .Journal of Forensic Science and Criminal Investigation. Vol. 2 pp.9-25.
76. Nsiah Amoako EN, McCartney C (2021). Swapping Carrots for Sticks: forensic science provider views of the Forensic Regulator Act 2021. Sci Justice. 2022; 62: 506-14.
77. Neware, R., & Khan, A. (2018). Cloud Computing Digital Forensic challenges. Proceedings of the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 29-31 March 2018, pp. 1090-1092. https://doi.org/10.1109/ICECA.2018.8474838.
78. Nakamoto S. Bitcoin:((2008) a peer-to-peer electronic cash system; 2008. Available from: https://bitcoin.org/bitcoin.pdf.
79. Nwafor (2017, November 27)Nigeria loses N127bn to cyber crime – Saraki . Retrieve from Vangaurd News: https://www.vanguardngr.com/2017/11/nigeria-loses-n127bn-cyber-crime-saraki/Accessed 25/6/2021
80. Okogba,E.(2018,May16).*News*.RetrievedfromVanguardNews:accessed6July,2018from www.vanguardng.com/newsAccessd 26/11/2020.
81. Okogba,E.(2018,April20).Vanguard News .Retrieved from Vanguard News: www.vanguardngr.comAccessd 26/11/2020.
82. OpenLearn. (2018, January 01). Digital Forensics. Retrieved from Open Learn: http://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3Accessd 26/11/2020.
83. OpenLib. (2018, January07). Open Library. Retrieved from Types of crime: Accessed 8 May, 2018fromhttp://open.lib.umn.edu/socialproblems/chapter/8-2-types-of-crime/Accessd 26/10/2020.
84. OSAC.(2017,July4).*Nigeria 2017 Crime and Safety Report: Lagos*. Retrieved from OASC: www.osac.gov/pages/contreportdetails.aspx?cid=21604Accessd 26/10/2020.
85. Petherick, W., Turvey, B., & Ferguson,C.(2010).London: Elsevier academic press availableat www.aboutforensics.co.uk/edmond-locard/. Accessed 26/11/2020.
86. Peter Oluka (2017, June 10). Guardian News Retrieved from https://guardian.ng/technology/communications/%E2%80%8Befcc-requires-computer- forensic- experts-to-win-cases-says-adeoye/ .Accessd 26/11/2020.
87. Prather, S. (2014, OCTOBER 6). when teens went missing digital forensics cracked case. RetrievedfromStartribune:http://www.startribune.com/when-teens-went-missing-igital-forensics-cracked-case/278132541/ Accessd 26/11/2020.
88. Prosise C., M and K (2003) Incident Response & Computer forensics, Second Edition .Mc Graw- Hill: New York.
89. Reith M., Carr C. & Gunsch G.(2002).An examination of Digital Forensic model .Department of electrical and Computer Engineering air force institute of technology. Write-Peterson.
90. Retrievefromwww.utica.edu/academic/institutes/ecii/ijde/articles.cfm?actionAccessd 26/11/2020.
91. Reuters, T. (2018,January9).FindLaw.RetrievedfromFindLaw:https://www.findlaw.com/Accessd 26/11/2020.
92. Rogers M.(2006) Digital Crime Scene Analysis model :applied digital crime scene analysis .In Tipton & Krause Vol. 1 pp. 298-299.
93. R.Ieong (2021) FORZA digital forensics investigation frameworkthat incorporates legal issues,Digital Investigation. Volume 3, Supplement 1. P 29 – 36
94. Rosenfeld,R.(2017,OCTOBER26).*ViolentCrime*.RetrievedfromCriminology-Oxford Bibliographies:http://www.oxfordbibliographies.com/view/document/obo- 9780195396607/obo-9780195396607-0001.xml Accessd 26/11/2020
95. Sarah V. Heart (2004) Forensic Examination of Digital Evidence .A guide for law enforcement.
96. U.S Department of Justice. National Institute of Justice Special report.Accessd26/11/2020
97. Singh, U., & Gaud, N.(2015).Analysis of the Digital Forensic Investigation Models .UDGAM VIGYATI, Volume 2, pp. 144- 149.
98. Stahl, B.(2008)Information Systems: Critical Perspectives. London:Rotledge8(6),66-78
99. Sunde N. Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations. Forensic science international. Digit Investig. 2022; 40: 301317.
100. Sundresan Perumal (2009) Digital Forensic Model Based on Malaysian Investigation Process.
101. *International Journal of Computer Science and Network Security*. Vol. 1. 9(8)pp. 98-103.
102. Tukur, S.(2018,February13).***News***. Retrieved from Premium times :
103. Tabona, A (2018) Top 20 Free Digital Forensic Investigation Tools for System Administrators. https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/
104. www.premiumtimesng.com/newsAccessd 26/11/2020
105. Unini Chioma (2021) T*he Nigeria Lawyer.com:* Alleged Revenge P*rn: Court Rejects WhatsApp Messages As Evidence In Trial Of Bayelsa Teenager.Retrieved from https://thenigerialawyer.com/alleged-revenge-prn-court-rejects-whatsapp-messages-as-evidence-in-trial-of-bayelsa-teenager/?utm_source=rss&utm_medium=rss&utm_campaign=alleged-revenge-prn-court-rejects-whatsapp-messages-as-evidence-in-trial-of-bayelsa-teenagerAccessd 26/11/2020
106. Vlachopoulos.K., Magkos S.E., and chrissikopoulous V.AModels for Hybrid Evidence Investigation International Journal of Digital Crime and Forensics 4(4):47-62. DOI: 10.4018/jdcf.2012100104