International Journal of Science Academic Research
Vol. 04, Issue 12, pp.6713-6722, December, 2023
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

DESIGN AND IMPLEMENTATION OF DIGITAL FORENSIC PROCESS MODEL FOR EFFECTIVE CRIME INVESTIGATION IN NIGERIA

***Onwubiko Davidson Chisom, Ukabuiro Ikenna Kelechi and Odikwa Henry Ndubuisi**

Department of Computer Science, Abia State University, Uturu, 441101

Received 14th October 2023; **Accepted** 20th November 2023; **Published online** 29th December 2023

Abstract

We are currently in an era of information, where digital devices and electronic communication have led to a high level of interconnectivity. These devices have become an essential part of our daily lives, and as a result, are often involved in criminal activities, making traditional crime investigation methods ineffective. The solution to this problem is a digital forensic model, which is required for effective crime investigation. Although there are already existing models globally, they are not specific to Nigeria's investigation process. Therefore, this work is focused on developing a digital forensic model based on Nigeria's investigation process and existing laws. This model is then implemented in software. The software has been analyzed and designed using the Object-Oriented Analysis and Design Methodology (OOADM).

Keywords: Forensics, Investigation, Crime, Model, Process, Evidence.

1. INTRODUCTION

Various crimes exist in Nigeria but lately, crimes such as terrorism, kidnapping, cybercrime, and rape have been on the rise, consequently, many people have lost their lives, wealth, jobs, and happiness in Nigeria. According to Okogba [1], over 1,351 people were killed in violent crimes between January and March 2018, while over 2 million people have been displaced from their homes [2]. Terrorist activities by the Boko Haram sect have resulted in over 100,000 deaths, injuries, and significant destruction of property since 2013 [2]. Boko Haram is widely believed to be the group responsible for a December 2014 prison break in Ekiti State, a bomb attack at an oil depot in Apapa Lagos, the Abuja Eagle square bomb blast, the Nyanya Abuja motor park bomb blast, etc [3]. Terrorism is a threat to the economy, political and social security of the nation, it discourages both local and foreign investments and reduces the quality of life. Kidnap for ransom (KFR) remains one of Nigeria's biggest challenges to date and has been a security concern nationwide [4]. In 2017, Nigeria was ranked 3rd on the global Internet crime index [5], and among the top ten countries for kidnap. Criminal organizations target affluent, high-profile Nigerians, and expatriates. In late 2016, kidnappers abducted 11 students and their teachers in Lagos. All victims were released following a ransom payment, but no kidnappers were arrested. Seven kidnappings involving U.S. citizens were reported in 2015. While none of these incidents resulted in the loss of life, substantial resources were used in their recovery [3]. In 2016, a Nigerian American was murdered near Owerri in an incident in which he was kidnapped for a brief period before being murdered [6]. Cybercrime is another crime affecting the socioeconomic well-being of Nigeria, it has given Nigeria a very bad image internationally. Cybercriminals have doubled their level of sophistication over the years, both government and non-government organizations in Nigeria lose millions of dollars to cybercriminals yearly. According to a statement released by the former senate president, Dr. Bukola Saraki, Nigeria has lost about 127 billion naira to cybercriminals as of November 2017 [7]. National critical infrastructures are been attacked by cybercriminals thereby jeopardizing the economic well-being of the nation. Digital forensics has not been largely used for solving crimes in Nigeria, moreover, where success is made with the current investigation approach years are gone, and as a result, many perpetrators go unnoticed. A typical example is the arrest of the leader of a notorious criminal gang in Nigeria, popularly known as Evans. For ten years, he had been on the most wanted criminal list in three different states- Edo, Anambra, and Lagos state. For years, he operated his syndicate under the radar; security agents had no idea where he lived or what he looked like, and was arrested after ten years by the Nigerian Police [8] Digital forensics may be applied while carrying out an investigation, but if the right procedure (digital forensic model) is not followed the outcome of such investigation may not be admissible in a court of law. A good example is the case of a serving Senator who was charged with rendering support to a terrorist group, the Boko Haram sect by the Federal Government, through a Chief State Counsel in 2011. The Chief State Counsel told the court that it garnered sufficient evidence that linked the accused to the terrorist sect [9] The prosecution later tendered proof of evidence that indicated that the accused person made contact with the Boko Haram sect 73 times. Some call logs and three digital video discs (DVDs), containing call-data records, as well as documents containing findings based on investigations carried out by the Department of State Security (DSS) were previously admitted into evidence by the trial court and were subsequently expunged from the trial record on the order of the Appeal Court in Abuja because the right digital forensics procedure was not followed in the acquisition of the evidence.

When digital forensics is applied in criminal investigation the result can be overwhelming as shown in the cases reviewed below.

Two Canadian teenage boys tortured, raped, and murdered a classmate, Kim Proctor after she dumped one of them via text message. While they burned her body, they were unable to

Corresponding Author:** ***Onwubiko Davidson Chisom,
Department of Computer Science, Abia State University, Uturu, 441101

eradicate the damning trail of evidence they left behind in the form of Wikipedia searches (for "lithotomy position" among others), instant messages, a confession in a World of Warcraft chat, GPS data associated with an "alibi" text message sent from the scene of the murder, and Google map searches for places to dump the body. Police bugged their homes, monitored their cell phones, and performed digital forensic analysis on their computers and phones. The boys pleaded guilty to first-degree murder and were sentenced to life imprisonment [10].

According to Dwan's report [11], John Diamond shot and killed Air Force Captain Marty Theer in December 2000 leaving no physical evidence or eyewitnesses. However, the prosecutors were able to get their hands on 88,000 emails and other messages on Michelle's computer including personal ads that Michelle had posted in 1999. They also found email responses from her for that ad which showed clear evidence of a sexual relationship between Michelle and Diamond. Furthermore, messages containing information about the conspiracy to murder Captain Marty were also recovered. On December 3rd, 2004, Michelle Theer was found guilty of murder and conspiracy and sentenced to life imprisonment.

According to Dwan [11], Scott Tyree kidnapped a 13-year-old girl named Alicia Kozakewicz. On the same night, Tyree sent a photograph of Alicia tied in his basement via Yahoo Messenger to someone in Tampa, FL. The man from Tampa happened to check the Pittsburgh Post-Gazette website and saw that the same girl was missing from her home. He then contacted the FBI on January 3rd and gave the FBI the Yahoo screen name of the person who had sent him the internet message (IM): '*masterforteenslavegirls*.' The FBI further contacted Yahoo and obtained the IP address from where the image was sent. They then contacted Verizon to obtain the name and address of the Verizon subscriber to whom the IP address was assigned. That person happened to be Scott Tyree.

Incorporating the right digital forensics procedure with the Nigeria Investigation process will surely produce similar results to the examples shown above. In Nigeria, when a crime is committed or ongoing it is often reported [12], where the complainant did not pen down the complaint, a provision is made for the documentation of the crime [13], then the crime is evaluated to identify the skills, tools and the documents [14] required for the investigation. The investigator gathers the evidence following the Evidence Act [15], and then the evidence obtained is examined /analyzed. A report is prepared [16] and presented to the jury or investigative panel for administrative purposes [14]. Finally, the evidence is returned to the owner at the end of the investigation and the report is Archived [13]. This process can be transformed into a digital forensic model that can be built into software.

The next section is a review of various forensics models existing around the world.

REVIEW OF EXISTING DIGITAL FORENSICS MODELS

Several digital forensics models exist around the world, most of which are developed to suit already existing laws. Most countries develop or adopt a digital forensics model based on their investigation process. This section will review some digital forensics models around the world, comparing them with the Nigerian investigation process.

Kruse and Heiser Digital Forensic Investigation Model

According to Singh & Gaud [17], computer forensics is a coherent application of methodical investigation techniques to solve crimes. Kruse & Heiser's investigation model consists of three phases namely: Acquiring, Authenticating, and Analysis.

1. Acquisition: At this phase, the digital evidence is collected in electronic format. This phase requires a high level of skill and expertise so as not to alter or damage the evidence.
2. Authenticating: digital evidence can easily be altered, hence this phase ensures that evidence is not tampered with in any form.
3. Analyses: the investigator at this level scrutinizes the evidence to get the facts that he or she is looking for.
4. This model is effective in maintaining the integrity of evidence. The second phase (authenticate), ensures the integrity of the evidence. However, it paid less attention to reporting which is a major part of Nigeria's investigation process.

Lee Scientific Crime Scene Investigation Model: This is an investigative model with four phases, namely: Recognition, Identification, Individualization, and Reconstruction.

1. Recognition, at this phase all the digital evidence is collected. An investigator collects as much digital evidence as he can at this phase.
2. Identification: This is the next phase after an investigator must have collected all the digital evidence, at this phase, the digital evidence relevant to the investigation is identified.
3. Individualization: This phase narrows down the digital evidence to the case being investigated.
4. Reconstruction: At this phase, the investigator links the digital evidence to the crime.

This model focuses more on the physical crime scene than the digital crime scene investigation. Preparation is omitted in this model. In Nigeria's investigation process, preparation forms part of the chain of custody, hence omitting it will jeopardize the admissibility of the evidence produced by this model.

Digital Forensics Research Working Group Model (DFRWS): This is a seven-phase model developed at the first digital forensics research workshop held by the Digital Forensics Research Working Group. The phases of this model are: Identification, Preservation, Collection, Examination, Analysis, Presentation, and Decision. Belonging to each phase are techniques to achieve the activities that take place in the phase.

1. Identification: in this phase, a computer-related incidence is identified. The incidence may be in progress or have already taken place.
2. Preservation: At this phase, an investigator preserves the digital evidence from being altered or destroyed.
3. The collection is the next phase which involves forensic duplication (aka imaging) of digital evidence using an approved procedure and standardized tools.
4. Examination: This is an in-depth search through the evidence.
5. Analysis: An investigator analyzes the evidence to link it with the crime being investigated.

6. Presentation: This is the summary and explanation of the conclusion drawn from the investigation. The presentation can be for an investigating panel or the jury.
7. The decision is made by the person(s) that the presentation is made to.

Documentation is not a phase in this model. Rather it is an activity in the Presentation phase. This model paid less attention to documentation by not making it an explicit activity in all the phases. In the Nigerian investigation process, when a crime is reported to a law enforcement agent, the agent is expected to document the crime before commencing an investigation.

Forensic Process Model: This is a four-phase model by the U.S. Department of Justice [18].The phases of this model are Collection, Examination, Analysis, and Reporting.

1. Collection: This involves searching for evidence, recognizing evidence, collecting, and documentation of evidence.
2. Examination: This phase involves examining the origin and the relevance of the evidence in a case. It involves revealing hidden and obscured information.
3. Analysis: This is where an investigator analyzes the evidence to link it with the crime being investigated.
4. Reporting: This is a documented summary of all steps taken for the investigation and the conclusion drawn from the investigation.

Though this model is basic and simple, it lacks other important steps such as preparation, and documentation.

Abstract Digital Forensic Model: This is a nine-phase digital forensic model that improved on the potential of the already existing DFRWS Model. The phases of this model are Identification, Preparation, Approach strategy, Preservation, Collection, Examination, Analysis, Presentation, and Return of Evidence [19].

1. Identification: This involves recognizing that an incident has occurred or is ongoing from indicators.
2. Preparation: This is the preparation of tools, techniques, and a search warrant for the investigation.
3. Approach strategy: This is the formulation of procedures and approaches to be used for the investigation.
4. Preservation: The investigator isolates, secures, and preserves the state of physical and digital evidence.
5. Collection: involves forensic duplication of the digital evidence using approved procedures and tools.
6. Examination: This is an in-depth search of evidence.
7. Analysis: This phase involves analyzing the evidence to link it with the crime under investigation.
8. Presentation: This is the summary and explanation of the conclusion drawn from the investigation.
9. Return evidence: Return physical evidence to the rightful owner.

The problem with this model is the arrangement of the phases since it is a linear process. In the Nigerian investigation process, the strategy to be used for an investigation is considered first before the preparation of tools to be used. In order words, the tools to be used for an investigation depend on the approach strategy chosen and not as prescribed by this model.

The Integrated Digital Investigation Process Model (IDIP): This is a 17-phase digital forensic model grouped into 5 phases namely: Readiness, Deployment, Physical crime scene investigation, Digital crime scene investigation, and Review [20]. This model converted the digital investigative process into the physical investigative.

1. Readiness: This phase ensures that an investigation is fully supported in terms of operations and infrastructure required. This phase has two sub-phases namely, operation readiness, and infrastructure readiness phase.
2. Deployment: This phase provides a mechanism for the detection and confirmation of an incident. It has two sub-phases namely detection and notification phase, confirmation, and authorization phase.
3. Physical crime scene investigation phase: This phase collects and analyzes the physical evidence and reconstructs the actions that took place during the incident. It has six sub-phases namely: preservation phase, survey phase, documentation phase, search and collect phase, reconstruction phase, and presentation phase.
4. Digital crime scene investigation phase: This phase collects and analyzes the digital evidence obtained from the physical investigation phase and the ones obtained through other future means. It has six sub-phases similar to that of the physical investigation phase (3^{rd} phase). However, the primary focus is on digital evidence. The six sub-phases are the preservation phase, survey phase, documentation phase, search and collect phase, reconstruction phase, and presentation phase.
5. Review phase: A review of the entire investigation is done and areas for improvement are identified. The problem with this model is distinguishing a digital crime scene from a physical crime scene. In Nigeria's investigation process when a crime is reported an investigator cannot categorically say that it is a digital or computer crime without carrying out a preliminary physical and digital investigation.

The Enhanced Digital Investigation Process Model (EIDIP): Florence Tushabe and Venansius Baryamruba [21] 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, Traceback, Dynamite, and Review. This model added two phases: the traceback, and dynamite.

Traceback is the 3^{rd} 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 4^{th} phase of this model. It investigates the primary crime scene (the computer). At this phase item found in the computer is 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 investigation.

Computer Forensics Field Triage Process Model

Some cases are time-sensitive, Roger et al. [22] identified the importance of time in investigating cases such as kidnapping,

Robbery, Terrorism, etc. He argued that the traditional models present at that time were 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 [22]. The phases of this model are derived partly from the Integrated Digital Investigation Process model [20] and partly from the Digital Crime Scene Analysis model [23].

Digital Forensic Model Based on Malaysian Investigation Process: Perumal [24] after studying the existing digital forensic models argued that none of the models focused on cybercrime investigation. He proposed a model that paid attention to fragile evidence and the data acquisition process [24]. This model has 7 phases namely: Planning, Identification, Recognition, Analysis, Result, proof and defense, and Diffusion of information.

1. Planning: this phase is subdivided into two phases namely: Authorization and search warrant. At this phase, authorization is obtained to empower or commission an investigator. A search warrant is also obtained before searching for evidence.
2. Identification: this phase is also subdivided into two, namely; identify the seized item, and identify fragile evidence. At this phase, the digital devices used by the suspect are identified and fragile data (live data) is identified.
3. Reconnaissance: An exploration is carried out to gather information from a system or network to carry out an investigation.
4. Transportation: the collected evidence has to be transported to a safer location where it will be handed over to an evidence custodian.
5. Analysis: An investigator or analyzer, analyzes the collected evidence. It is important to note that not all the evidence can provide all the proof that an investigator is looking for, but can provide a lead.
6. Proof & defense: The reason for an investigation is to prove or disprove a claim, hence at this phase an investigator proves and defends the validity of the case using his findings.

7. Archiving storage: After the investigation, the evidence is stored for future reference. This model focused much on live data acquisition (fragile or volatile data) and paid less attention to forensic duplication which is not spelled out like in the case of live data acquisition which is mentioned as a sub-phase in phase 2 [22]. The Nigeria investigation process requires that an investigator makes a forensic duplicate (forensic image) for analysis

THE NEW DIGITAL FORENSIC MODEL

This model is named Extended Forensic Process Model (EFPM), it is based on the Nigeria investigation process. This model is implemented in software named: Extended Forensic Process Model Application (EFPM App). The model as the name implies extended the four phases of the Forensic Process Model (FPM) as shown in Fig. 1a to eleven phases as shown in Fig. 1b. The phases are: Planning, Identification, Documentation, Collection, Packaging and Transportation, Examination, Analysis, Reporting, Presentation, Archiving, and Return evidence.

Figure 1a: Forensic process model

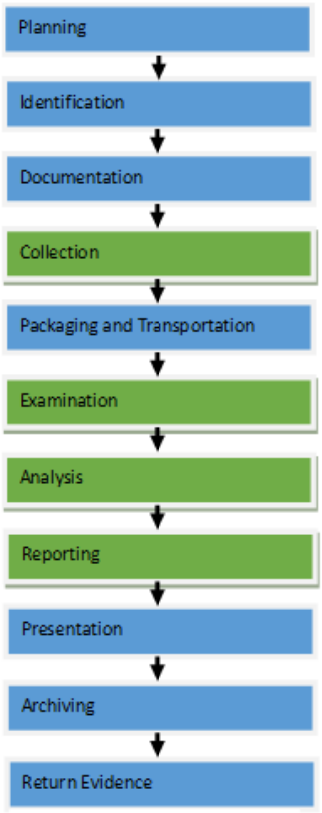

Figure 1b: Extended Forensic process model

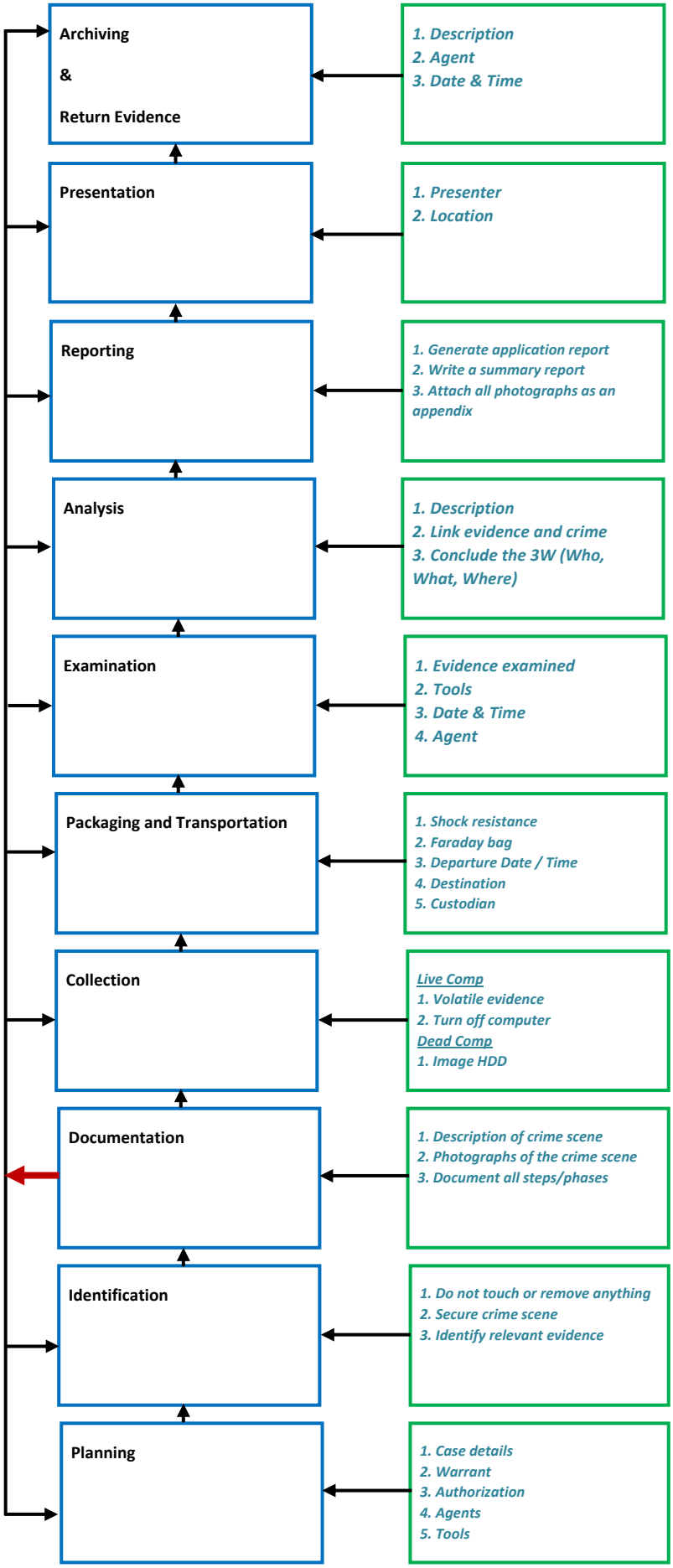

Figure 2. The Extended Forensic Process Model with all the activities in each phase

1. Planning: When an incident occurs, an individual or team is assigned to such an incident to ascertain what happened, when it happened, and where it happened (3W) hence it is called an incident response. The first step in incident response is planning. Planning involves getting an authorization/ search warrant before going to a crime scene. In the Nigerian investigation process, an investigator cannot go to a crime scene to search or seize any item without having a search warrant, otherwise, the outcome becomes null and void. Planning is the first phase in the extended forensic process model, at this phase, an investigator acquires all the legal documents required to carry out the investigation. This phase ensures the admissibility of the outcome of the investigation by ensuring the following:

i) That the investigator is legally authorized to carry out the investigation.
ii) That the investigator presented a search warrant permitting the search and seizure of evidence at the crime scene.

Planning forms part of the chain of custody. It takes place before the investigator gets to the crime scene.

EFPM APP Activities

i. The App prompts the investigator to input the following case details: Case name, Name of the person that reported the incident, Incidence date, and time.
ii. The App prompts the investigator to upload the search warrant and authorization letter.
iii. The App brings out a list of suggested agents and asks the investigator to select agents to form members of the team.
iv. The App brings out a list of suggested tools and asks the investigator to select suitable tools.

2. Identification: According to Locard's exchange principle, the perpetrator of a crime will bring something into the crime scene and leave with something from it, and both can be used as forensic evidence [25]. Often there is much evidence in a crime scene, both relevant and irrelevant to the investigation. In the Nigerian investigation process, an investigator is required to gather relevant evidence that can help in the investigation. The second phase of the Extended Forensic Process Model is identification. In this phase, the investigator identifies evidence relevant to the case under investigation. Identification of relevant evidence reduces the unnecessary time spent on the investigation, thereby making the investigation efficient.

EFPM APP Activities

i. The App warns the investigator not to touch or remove anything at the crime scene.
ii. The App instructs the investigator to cordon off perimeters of the crime scene.
iii. The App prompts the investigator to enter the list of identified evidence and tag them with serial numbers.

3. Documentation: This phase ensures that both the evidence identified and the crime scene are fully documented. This phase primarily promotes accountability. To further ensure the admissibility of the evidence, it is advisable to take photographs of the crime scene without touching or removing anything at the crime scene. Document how you met the crime scene, and make sketches where necessary. In the case of a digital device, document the condition of the device, name, make, model, and serial number of the device. Documentation is very important in the Nigerian investigation process, it forms part of the chain of custody, and it promotes the integrity of evidence. Hence it has been added as a phase in this model.

EFPM APP Activities

i. The App prompts the investigator to enter a brief description of the crime scene.
ii. The App instructs the investigator to take a photograph of the crime scene and attach it as an attachment.
iii. The App encourages the investigator to document all steps.

4. Collection: This phase is called the evidence acquisition phase. This phase takes into consideration all the necessary precautions to ensure that the evidence is not contaminated in any way. In the Nigerian investigation process, once evidence is contaminated or altered, the evidence becomes inadmissible. This phase ensures that evidence is not altered or destroyed during acquisition. It highlights key things an investigator should avoid to ensure that evidence is not altered. The under-listed are major provisions of this phase:

i. Never make direct contact with physical evidence without wearing a hand glove.
ii. Clearly label all the evidence.
iii. In the case of a computer system, if it is "ON", don't turn it "OFF" until all the volatile data is acquired. If it is "OFF" do not turn it "ON", then remove the hard drive and proceed with data acquisition.
iv. Never perform examination or analysis directly on a hard disk, instead, make a forensic duplicate (image) of the hard disk. While making an image of a hard disk ensure to use a write blocker and an appropriate imaging tool. Ensure the integrity of the image using a hash value.
v. in the case of a mobile phone, if it is "OFF" turn it "ON", if it is "ON" leave it "ON" and exclude it from the network using a Faraday bag, then proceed with data acquisition (Physical, and Logical extraction).

EFPM APP Activities

Live Computer (System that is Powered ON)

i. The App carries volatile data acquisition. The volatile data acquired at this stage are System date and time, running applications, open ports and applications listening on them, running processes, and process IDs.
ii. The App instructs the investigator to shut down the system.

Dead Computer (System that is Powered Off)

i. The App instructs the investigator to remove the hard disk.
ii. The App calculates the hash value of the hard disk and images the hard disk
iii. The App recalculates the hash value and compares it with the first calculated hash for authentication.
iv. The App prompts the investigator to enter the name of the evidence.
v. The App prompts the investigator to enter the name of the tools used for imaging.
vi. The App prompts the investigator to enter the date and time of the imaging
vii. The App prompts the investigator to enter the name of the agent that performed the imaging.

5. Packaging and Transportation: Examination and Analysis are often done at the laboratory, hence the evidence needs to be properly packaged and transported to the laboratory. During this phase the evidence should be packed in a container that will not allow much shock on the evidence, the container should be heat-resistant and waterproof. When the evidence arrives at the destination it should be handed over to an evidence custodian who will take note of the arrival of the evidence before moving it to the laboratory for examination and analysis.

EFPM APP Activities

i. ***Laptop and Desktop:*** The App instructs the investigator to pack the evidence in a shock resistance box.
ii. ***Mobile Phone:*** The App instructs the investigator to pack the mobile phone in a Faraday bag to exclude it from the network.
iii. The App instructs the investigator to enter the departure date time, and destination.
iv. The App instructs the investigator to enter the details of the evidence custodian

6. Examination: in this phase, the collected evidence is processed and examined using the appropriate forensic tool. An in-depth system search is done on the evidence, and hidden and obscured files are recovered in this phase. All evidence is thoroughly examined according to the nature of the crime. A keyword search related to the crime using regular expression (Regex) is done. Deleted data and Metadata are goldmines in an investigation, hence they are not overlooked by this phase. This phase also paid attention to all log files and system files. A criminal may want to cover his tracks by deleting some files, an investigator should go through unallocated space of the image file to undelete or recover as many files or file fragments as possible. Ensure to decrypt all encrypted files. Perform a string search to help in the analysis phase. Identify all compressed files and decompress them.

EFPM APP Activities

i. The App instructs the investigator to enter the name of the evidence under examination.
ii. The App attaches the image of the evidence to be examined and commences the examination.
iii. The App prompts the investigator to enter the date and time of the examination.
iv. The App prompts the investigator to enter the name of the agent that performs the examination.

7. Analysis: In this phase, the results of the examination are analyzed to link the evidence with the crime being investigated and draw a conclusion based on the evidence found. Timeline is important in this phase, an investigator should take note of the time/date stamp of important files. Last written and modified time/date stamp, creation time/date stamp, and last access time/date stamp are very important in investigation and are used for linking file(s) to the crime under investigation.

EFPM APP Activities

i. The App prompts the investigator to enter a description of the examination.
ii. The App prompts the investigator to link the evidence with the crime under investigation.
iii. The App prompts the investigator to conclude who, when, and where.

8. Report: The investigation aims to prove or disprove a claim. In the Nigerian investigation process, the report is very crucial. This phase document fact and/ or offers opinion with a style of communication that provides decision-makers with useful, accurate information. An investigator should write his report in such a way that decision-makers will understand the content clearly. An investigator should have a standard way of reporting an investigation, it should include all the steps on how the investigation was carried out and how the conclusion was drawn. A computer forensic report should achieve the following:

i. Accurately describe the details of an incident.
ii. Understandable to decision-makers.
iii. Able to withstand legal scrutiny.
iv. Unambiguous and not open to misinterpretation.
v. Be easily referenced (using paragraph numbers for the report and Bates numbers for the attached documents).
vi. Contain all information required to explain your conclusions
vii. Offer valid conclusions, opinions, or recommendations when needed.
viii. Be created on time.

EFPM APP Activities

i. The App generates a report.
ii. The App instructs the investigator to manually write a report.
iii. The App instructs the investigator to attach all photographs as an appendix.

9. Presentation: At the end of an investigation, the report is often presented to an investigative panel or judge(s). This phase allows an investigator to appear before a panel or judge(s) to present his findings. S.68 (1) and S.68 (2) empower an expert to appear before a judge to give his opinion as an expert witness.

EFPM APP Activities

i. The App prompts the investigator to enter the name of the agent to present the report.
ii. The App prompts the investigator to enter the location where the report will be presented.

10. Archiving: The Nigerian legal system made provision for parties to appeal their case if they are not satisfied with the judgment. This phase ensures that images of the digital evidence and the report are safely stored for future reference.

EFPM APP Activities

i. The App prompts the investigator to enter a description of how the image and the report are archived.

11. **Return evidence:** This phase ensures that at the end of the investigation, the physical evidence is returned to the owner.

EFPM APP Activities

i. The App prompts the investigator to enter the name of the agent that returned the evidence to the owner.

ii. The App prompts the investigator to enter the date and time the evidence was returned.

ANALYSIS OF THE EXTENDED FORENSIC PROCESS MODEL APPLICATION (EFPM App)

User Requirement Analysis: A user of this system will have expectations, these expectations are classified as functional and non-functional requirements.

Functional Requirement: This relates directly to the processes the system must perform:

i) Login: The users of the system (both the Admin and the investigators) should be able to log into the system by providing the correct password. An Admin is a superuser of the system and, hence will log in with higher privilege. An investigator is a normal user of the system and, hence will log in with lesser privilege.
ii) Create Account: only the Admin should be able to create an account in the system. The account created by the Admin is normal, the investigator can log in with this account.
iii) Create Case: Only an investigator should be able to create a new case in the system. An investigator can create as many cases as he/she wants.
iv) Update Case: when an investigator wants to revisit an existing case he/she should be able to retrieve and update it. Only an investigator can update the case
v) Print Report: An investigator should print a summary of the case as a report
vi) View cases: Both the Admin and investigator should view the number of cases created and the case details.

Non-functional Requirement: This refers to the behavioral properties that the system must have such as usability and performance:

i) The investigator must change the initially assigned login password immediately after the first successful login. The initial password should never be reused.
ii) The system should handle multiple investigators working at the same time without affecting the system's performance.
iii) The system should be easy to learn and easy to use.

Use Case and Domain Analysis: The use case diagram in Figure 3 describes in more detail the key elements of the requirement definition. It presents the different users of the EFPM App and what each user does with the system. The users are referred to as actors. Below are the actors and how they interact with the system.

1. **Admin:** A super user of the system with the highest privilege. An Admin can log in, create a user account for an investigator, remove the investigator from the system by deleting the account, search for a case using the case ID, view cases created by all investigators, and log in. However, Admin cannot create or update cases.

2. **Investigator:** A normal user of the system. An investigator login to the account created by the Admin with the login details provided, and changes the password through the account settings option, Create Case, Search Case, View Case, Update Case, Create Report, and logout.

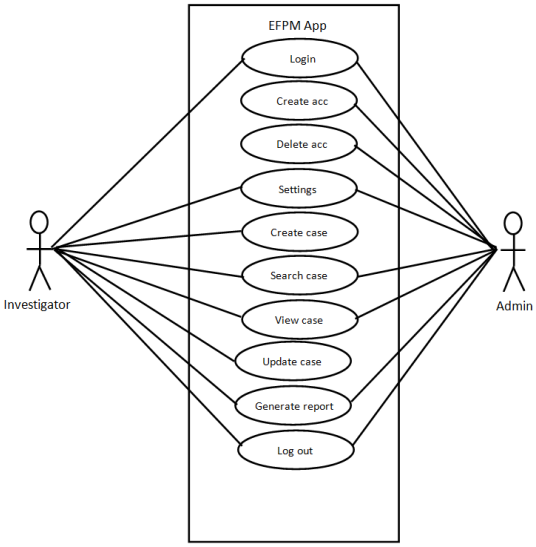

Figure 3. Use Case diagram of EFPM App

Sequence diagram: Figure 4 depicts a series of activities that take place from the time of login to logout of the EFPM App. Users log in to the system by entering a username and password, the system validates the type of account, and each account has a privilege right assigned to it. If the account is Admin, the Admin creates a user account for an investigator and performs other activities. If the account is an investigator's account, the investigator creates a case using the EFPM.

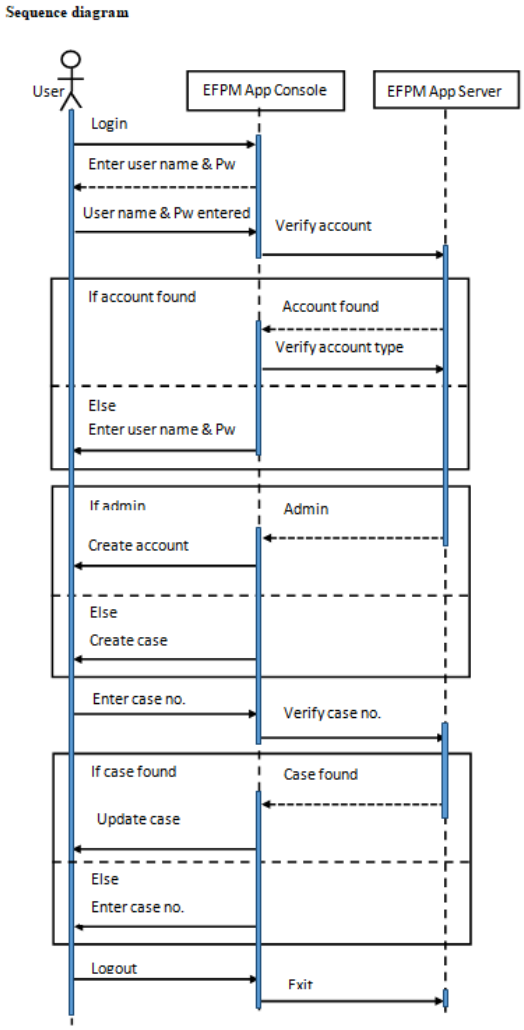

Figure 4. Sequence diagram

SYSTEM DESIGN

Here, the data that was gathered during the analysis is used to create the blueprint for the new system. This is followed by System implementation which focuses on building the system, ensuring that it performs as designed.

Architectural Design

The EFPM App adopts a thin Client-server architecture [26]. The three primary components of the system are client computers, servers, and the network that connects them.

The Client will be responsible for the presentation logic that displays information to the users and the acceptance of the user commands (the user interface). It will also contain only minimal (thin) application logic using such programming languages as JavaScript.

The Server is responsible for the data storage and data access logic (the database queries are in Structured Query Language (SQL)

Hardware and Software Specification

The hardware and software specification is a document that describes what hardware and software are needed to support the application. Hardware and software specifications for the new system are outlined below.

Hardware Requirements

For efficiency, the server on which the software is installed should have; an x64-based PC, Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz, 2100 Mhz, 2 Core(s), 4 Logical Processor(s), Physical Memory (RAM) of 4.00GB, total Physical Memory of 3.94GB, Total Virtual Memory of 7.87GB and Hard disk drive of 4 Terabytes. The client system is preferred to be always on Broadband and Dual 100 Mbs Ethernet for the web server of 10 Mbps

Software Requirements

The system will operate on all common platforms namely Windows, UNIX, Macintosh, and Solaris. The system will operate in a Hypertext processor (PHP) environment for the server side, a web browser preferably Mozilla Firefox or Google Chrome for the client side, and Windows, Apache, My-SQL, and PHP (XAMPP) as web browsers.

Input Form Design

This is the design of input screens used to accept data from the user into the EFPM App. The type of inputs used in this design are text fields, number fields, and drop-down list boxes.

Input Validation

This was achieved using Javascript & PHP scripts. All data entered into the system are validated to ensure accuracy. The system does not accept data that fail any important validation check to prevent invalid information from entering the system. The system identifies invalid data and notifies the user. The validation checks used are completeness check, format check, consistency check, and database check. Completeness check ensures all required data have been entered. Format check ensures data are for the right type (e.g., numeric, e-mail) and in the right format (e.g., month, day, year) consistency check ensures combinations of data are valid, (e.g., in the case of new password and confirm password). Database checks compare data against a database to ensure they are correct. The user's username and password are compared against a database.

Output Query result format

The goal of output query results is to present information to users so they can accurately understand it with the least effort. Outputs in the EFPM App are the reports the system produces.

Interface Evaluation

Interface evaluation was done while the system was being designed so that any major design problems could be identified and corrected before time. An interactive evaluation was conducted by the researcher and the potential users. As the user interacts with the prototype, the researcher records the situation when the user appears to be unsure of what to do, makes mistakes, or misinterprets the meaning of an interface component. Several minor changes were identified and modifications were made to the user's satisfaction.

SYSTEM IMPLEMENTATION

Choice of Implementation Tools/ Languages: Different web application languages and modeling tools were used for the design and implementation of the EFPM App. These included the following; Hypertext Markup Language (HTML), Hypertext Preprocessor (PHP), MYSQL, Cascaded Style Sheet (CSS), JavaScript, Dream Weaver, Fireworks, SWiSHmax, and Visual Paradigm. Graphical user interfaces are generated using Dream Weaver which is a HTML-based application. The visual editing feature of the Dream Weaver allows the creation of a web page without having to type HTML code. It supports graphics created by Fireworks or any other application to be easily imported to the web page. It also provides a coding environment with coding tools for users to edit HTML codes or to include any other scripting language. The scripting language behind the development of the EFPM App is PHP. Other Scripting languages used are CSS and JavaScript. JavaScript is used to add functionality beyond standard HTML to a web page. It adds interactivity to the website. Visual Paradigm application was used to draw the UML diagrams. The researcher's choice of PHP and MySQL for this project is because of the benefits it offers. Such as it is open-source, and it completely separates content from the designing part. This way you only need to update the database and the rest is taken care of by the system [27]

Database Management System (DBMS) Implementation: The database server that was adopted for the project is the MYSQL database server. This is mainly because of its easy interaction with PHP-enabled web servers, the ability to serve many parallel client requests, and its secured nature (Secured Socket Layer (SSL) and SSH security plug-ins). It is also affordable (it is open-source when used for academic and research purposes). The web server software chosen for this project was the XAMPP (Cross-Platform, Apache, Mysql, PHP, and Perl). This is because it can be used on any platform, it is robust, and it is open source. The DBMS described above entailing web browsers like Mozilla Firefox, Google Chrome,

Internet Explorer, web server, and database server, provides sufficient security functionality, works well in a multi-user environment, and is stable with large volumes of data.

Figure 5 shows the admin login page and the admin dashboard of the EFPM App. Figure 6 shows the agent login and Dashboard of the EFPM App

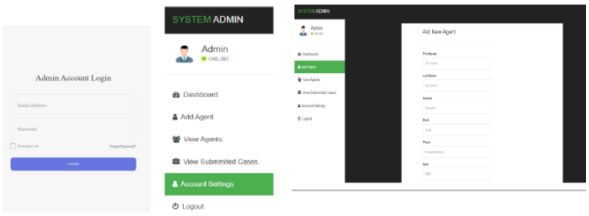

Figure 5. Admin login and Dashboard of EFPM App

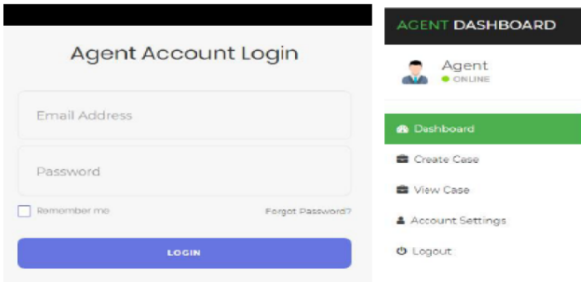

Figure 6. Agent login and Dashboard of EFPM App

CONCLUSION

Incorporating digital forensics in a criminal investigation as shown in the introductory part of this work has helped in solving complex crimes around the world. However, the practice cannot be complete without a model to guide an investigator on what to do and how to do it. Hence the EFPM will serve as a good guide for effective crime investigation in Nigeria. Furthermore, the EFPM App as shown in Figures 6 and 7 will guide an investigator through the model. In conclusion, this digital forensic model implemented in the software will enforce uniformity and increase accuracy in the investigation process, above all reducing the crime rate in Nigeria.

REFERENCES

1. Okogba, E. (2018, May 16).Vanguard News.[Online] Available: www.vanguardng.com/news. [Accessed Dec. 1, 2023].
2. Tukur, S. (2018, February 13). Premium Times.[Online]Available:www.premiumtimesng.com/news .[Accessed Dec. 2, 2023].
3. OSAC. (2017, July 4). *Nigeria 2017 Crime and Safety Report: Lagos*. [Online]Available: OASC: www.osac.gov/pages/contreportdetails.aspx?cid=21604 [Accessed Dec. 2, 2023].
4. Cunningham, A. (2018, January 29). CBC News. [Online]Available: www.cbc.ca/amp/1.4507272 [Accessed Nov. 10, 2023].
5. Jannah, C. (2017, August 22). *Daily Post Nigeria News*. [Online]Available: www.dailypost.ng/2017/8/22 [Accessed Nov. 10, 2023].
6. Okogba, E. (2018, April 20). *Vanguard News*. [Online]Available: www.vanguardngr.com [Accessed Nov. 23, 2023].
7. Vanguard. (2017, November 6). Vanguard *News*. [Online] Availablewww.vanguardngr.com/2017/11/nigeria-loses-n127bn-cyber-crime-saraki [Accessed Nov. 23, 2023].
8. Intelligence, B. (2017, July 6). *bulwarkintelligence*. [Online]Available:http://www.bulwarkintelligence.com/reports/crime/best-way-solve-crime-nigeria-offer-money [Accessed Nov. 25, 2023].
9. Nnochiri, I. (2017, June 7). Vanguard*News*. [Online] Available:https://www.vanguardngr.com/2017/06/boko-haram-sponsorship-ndume-case-answer-fg-tells-court-2 [Accessed Nov. 25, 2023].
10. Hill, K. (2011, November 3). Forbes: [Online]Available: https://www.forbes.com/sites/kashmirhill/2011/11/03/solving-a-teen-murder-by-following-a-trail-of-digital-evidence/#36bb03b61833 [Accessed Nov. 26, 2023].
11. Dwan, C. (2018, January 4). *Notable Computer Forensics Cases*.[Online]Available:Institute:ttps://resources.infosecinstitute.com/category/computerforensics/introduction/notable-computer-forensics-cases/#gref[Accessed Nov.26, 2023].
12. Administration of Criminal Justice Act 2015, 88(1)
13. Administration of Criminal Justice Act 2015, 89(1)
14. Associate, Dewpoint Legal Practitioners. 27 October 2017. Correspondence with Research Directorate.
15. Evidence Act 2011
16. Nigeria. 31 October 2017 Police Force, Special Fraud Unit. Correspondence from a Police Public relations officer to the Research Directorate.
17. Singh, U., & Gaud, N. (2015). Analysis of the digital forensic investigation models. *UDGAM VIGYATI, Volume 2*, 144- 149.
18. Sarah V. Heart (2004) Forensic Examination of Digital Evidence. A guide for law enforcement. U.S. Department of Justice. National Institute of Justice Special report.
19. Reith M., Carr C., Gunsch G. (2002). An examination of the Digital Forensic model. Department of Electrical and Computer Engineering Air Force Institute of technology. Write-Peterson. [Online]Available: www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action [Accessed Nov. 27, 2023].
20. Brian Carrier and Eugine H. Spafford (2003) getting physical with the investigation process. *International journal of digital evidence.* 2(2)
21. Baryamureeba, V., & Tushabe, F. (2004, August). The enhanced digital investigation process model. In Proceedings of the Fourth Digital Forensic Research Workshop (pp.1-9).
22. Rogers M. (2006) digital crime scene analysis model: applied digital crime scene analysis. In Tipton & Krause
23. Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota (2006). Computer forensics field triage process model. *Journal of digital forensics, security and Law.* Vol1 (2)
24. Sundresan Perumal (2009) Digital Forensic Model Based on Malaysian Investigation Process. *International Journal of Computer Science and Network Security*. 9(8)
25. Petherick, W., Turvey, B., & Ferguson, C. (2010). Forensic Criminology. London: Elsevier accademic press available at www.aboutforensics.co.uk/edmond-locard/.
26. F. Jerry, D. Alan, "Architectural Design. Business Data Communications and Networking", 6th Ed. John Wiley & Sons, Inc. pg. 76, 1999.
27. Ajah I.A &Inyiama H.C. (2013). A Model of DNS-Based Bank Credit Risk Management System in Nigeria. *ARPN Journal of Systems and Software*, 3(6).

****