ISSN: 6228 - 3548
Volume 10, Number 2, 2024
International Journal of Applied and Physical Science Research

DIGITAL FORENSIC: A PANACEA FOR CRIME DETECTION IN NIGERIA

Nachanuya Suleiman
Department of Computer Science and Information Technology, Igbinedion University, Okada, Edo State, Nigeria

nachanuyasuleiman@mail.com

ABSTRACT

Digital forensic is the fastest evolving field of computing that bridges the gap between science and legal process of investigation. Digital forensic consists of computer forensics, network forensics, mobile forensics, cloud computing forensics, and IoT forensics; and for this reason have digital evidence distributed widely when the need arises for crime prosecution. In the application of digital forensic, the need for authenticity, accuracy, completeness and convincing digital evidence is the vital point of view by the court for proper legal action. This study hence provides the concept and suggestive digital forensic model and also the solution to unsolved or lingering crimes perpetrated in Nigeria. It is noticed that, cyber crimes are diversifying in its sophisticated modules where the miscreants are almost invincible to arrest because there is a deficiency in the investigative system, but the invent of digital forensic, there will be a drastic solution to such crimes. For the study to be relevant to policy and practice, forensic tools and frameworks, legal and ethical obligations, and digital evidence handling and admissibility are highlighted. This paper does not follow any forensic investigations process; but rather discusses the need for development and implementation of unique frameworks that could be utilized to gather distributed digital evidence required for admissibility in court.

Keywords - Digital forensics investigations; Digital evidence; Jurisprudence

INTRODUCTION

According to the scholar; Joseph (2018), he suggested a definition to digital forensics as "the application of scientifically established methods in preserving, collecting, validating, identifying, analyzing, interpreting and presenting digital evidence to the court of law after obtaining the evidence from reconstruction of events if possible". It was recorded that in the late 1990s and early 2000s was the inception of computer based crime as its growth started with the increased usage of computers and the Internet or internet based devices. Digital forensics developed as an independent field (Sriram Raghavan). The field is made up of computer forensics, network forensics, mobile forensics, cloud computing forensics, and internet of things (IoT) forensics.

There are various phases largely field in digital forensic that explain the distributed nature of evidence to be collected when a computer/cybercrime is reported or suspected to have been perpetrated. Citing the evidence law, "digital evidence or electronic evidence is any probative information that's stored or is being transmitted in digital form that a party to a court case may use at trial". As suggested by Ryan, "for evidence to be admissible in court, it must be relevant, material and competent, and its probative value must outweigh any prejudicial effect". This paper is targeted at giving the suggestive idea of the panacea to crime detection in Nigeria as the present state of investigation is still the traditional method of crime fighting and investigation. As stated earlier, this study focuses on the frameworks for gathering distributed digital evidence that can meet the techno-legal requirements for admissibility in the courts of law.

Background to the Study

Dated to the history of computing, digital forensics is the most closely defined by legal requirements, and its growth and evolution is informed and guided by case law, regulatory

changes, and the ability of cyber-lawyers and digital forensics experts to take the products of forensic tools and processes to court (Ryan, 2000).

Studies by scholars like Khanafseh & Qatawneh, 2019; shows that traditional forensics is based on the evidence of a tangible entity that could identify the criminal, such entities as blood, fingerprint, and hair, but these evidences cannot be found at digital forensics. The laws courts resort to digital evidence have increased in the past few decades.

Hence the permission by the court to use e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, internet browser histories, databases, digital printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files found on digital devices such as computers, external hard drives, flash drives, routers, smart phones, tablets, cameras, smart televisions, Internet-enabled home appliances; and communication service providers business records; and cloud storage providers records of user activity and content as evidence against the accused or criminal was made possible, thereby permitting digital forensic to actualize its perfection in dynamic crime detection. Related to the rise and use of several electronic means of transfer of documents and information, especially with the commission of cybercrime, this went beyond national and continental boundaries; hence distributing evidence and making information and database collection ring process a stressful task.

Related Literature

This literature review was adopted as a research methodology in order to be handy with the existing reviews relevant to the study.

Forensic Tools and Frameworks

Digital forensic is a specialized field of computing that aids the investigator with platform to gather evidence, to analyze them, and this is possible via the application of unique tools. As Patil & Devane (2022) have proposed a network forensics protocol that ensures tracking up to the true source of digital evidence by collecting beforehand forensically sound evidence and the protocol can collect target data from the device in the form of a device fingerprint. On the other hand, Joseph (2018) began an implementation of a digital forensic framework that could be used with standalone systems as well as in distributed environments, including cloud systems. This idea was derived towards combining concepts of cyber forensics and security frameworks in operating systems. Where Khanafseh & Qatawneh (2019) went on to conduct a survey of various frameworks and solutions in all branches of Digital Forensics in view of Cloud Forensics which then concluded to a solution as to improve many key issues such as security, accuracy, performance and privacy as vital issues to be considered in the framework. With the operation of Cyber offenders that's in fast spread as the rate at which the Internet and cloud computing is developed; hence it worsen the challenges in the collection and analysis of digital evidence in a cybercrime investigation. Establishing timeline information using date-time stamps is recommended for law enforcement agents in investigating cloud-related crime (Kao, 2016).

Legal and Ethical Obligations

Despite the availability of some forensic tools and frameworks, there is always the need to assess the legal counsel in the utilization of these frameworks in the gathering and harmonizing distributed evidence for purpose of administering justice in the court of law.

According to the (International, N.D.) "When a case is identified to have evidence distributed across geographical boundaries – legal frameworks and human rights information about jurisdictions come into play. It therefore becomes imperative to identify country-specific laws and cultural norms that may affect the investigative process and also determine whether additional subject-matter or local professionals will be needed". There are several applications, websites, and digital devices that utilize cloud storage services mainly for saving data as the

distribution of user data is done in fragments by different cloud service providers in servers to multiple locations (Practices & Acquisitions, 2018).

To retrieve such data from these providers is quite a difficult task and therefore the need to resort to International Cooperation against Cybercrime framework which is the digital forensic.

Digital Evidence Handling and Admissibility

Digital evidence is very volatile and fragile therefore it requires a proper and meticulous handling to avoid alteration by malicious miscreant, hence the careful handling of it is a paramount determinant to jurisprudence. As stated by (Standard & Last, 2018), there are four phases involved in the initial handling of digital evidence and these are: identification, collection, acquisition, and preservation must be adhered to. Therefore it is also necessary to note that in the course of handling digital evidence, certain legal and technical requirements must be met to ensure the admissibility of the evidence in a court of law (Antwi-boasiako, 2018).

Going by the assertions of AY & Akoto (2020), it's clear that for digital evidence to be admitted in the court of law while presented, it's authenticity, accuracy, complete, and convincing to the jury. Antwi-boasiako, (2018) advices that in order to proceed with the provision of such evidence obtained from digital forensic for admissibility, there is a need that the court examines the legal authorization to conduct searches and seizures of information and communication technology and related data, and the relevance, authenticity, integrity, and reliability of the digital evidence.

Implications for Cyber Safety in Nigeria

With the rise cyber crimes and its sophistication modus operandi of these miscreants, a developing nation as Nigeria needs to understand the proper and dynamic needs of cyber security. The areas to be well spelt as a loop hole for cyber crime in Nigeria are:

a. Cybercrime Threats: Nigeria is faced seriously with the high challenge of cyber crimes which is operational is several ways or methods by the miscreants and such methods are: hacking, identity theft, phishing, ransom ware attacks, and online fraud. These acts pose threats to national security and can result in significant financial losses, personal data breaches, and reputational damage to individuals, businesses, and the government.
b. Economic Impact: what Nigeria need at this time of economic quagmire is the advance implementation and application of digital economy, and the success of this to be in play, the cyber space must be safe for operations, because with a successful cyber attack there will be a disruption of online transactions, compromise financial systems, and hinder economic growth. Hence, protecting critical infrastructure, financial institutions, and businesses from cyber threats is vital for sustaining Nigeria's economic development.
c. Government Systems and Data Protection: Nigeria as sovereign country, conceal classified data and information which includes citizen information, critical infrastructure systems, and national security assets. Therefore securing the cyber space is paramount.
d. Personal Data Privacy: As more Nigerians embrace digital services, personal data privacy becomes paramount. Cyber security measures help protect individuals' personal information, ensuring that it is not unlawfully accessed, misused, or sold. Data breaches can lead to identity theft, financial fraud, and other forms of cybercrime that can have a severe impact on individuals' lives.

To every presented challenge, there lays a solution to be suggested if critically looked into. Hence below are some vital suggestions:

i. Legislation and Regulations: it is a suggestion for a developing sovereign nation as Nigeria to develop and implement with the sense of urgency a comprehensive cyber security laws and regulations that define responsibilities, establish standards, and outline consequences for cybercriminals.

ii. Capacity Building: institutionalizing cyber security by investing in cyber security education, training programs, and research initiatives to develop a skilled workforce capable of effectively preventing, detecting, and responding to cyber threats.
iii. Public-Private Partnerships: Encouraging collaboration between government agencies, private organizations, academia, and civil society to share information, resources, and best practices in cyber security.
iv. Incident Response and Cyber Threat Intelligence: Establishing effective incident response mechanisms and cyber security information sharing platforms to enable timely detection, response, and mitigation of cyber threats.
v. International Cooperation: Collaborating with international partners, organizations, and law enforcement agencies to combat transnational cybercrime, share intelligence, and enhance cyber security capabilities.

Guideline Model for Digital Forensic Investigation

Establishing the fact that digital forensics is the science of acquiring, retrieving, preserving and presenting data that has been processed electronically and stored on digital media. Being it a newly introduced discipline, digital forensic science has the potential to greatly affect specific types of investigations and prosecutions (Asian School of Cyber Laws 2006; Hall & Wilbon 2005). To perform the operations involved to digital forensic, a model is necessary needed to be designed where the organizations willing to provide this service must be capable of providing the means that helps an organization to be prepared to detect and counter cyber crime incidents in a skilled and efficient manner. This suggested model has operational entities as the combination of technically skilled people, policies and tool development.

This model depends on previous existing models as well as physical forensic models so that it can meet the challenges from the nature of electronic evidences to make it admissible in courts. To meet these challenges follow the forensic procedures proposed in this paper in which it can be applied for any case according to but not limited to these five phases these phases, knowing that each phase can change according to the case nature.

Existing Models

There are several models for investigation, most of them restrict themselves in the investigation of the crime scene and evidence and does not represent a detailed steps that can be used in guiding investigators. Some of these models are:

i. The U.S. Department of Justice published a process model in the Electronic Crime Scene Investigation: A guide to first responders (National Institute of Justice 2001) that consists of four phases: Collection, Examination, Analysis and Reporting.
ii. An Abstract Digital Forensic Model (Reith & Gunsch 2002) proposes a standardized digital forensics process that consists of nine components: Identification, Preparation, Approach strategy, Collection, Examination, Analysis, Presentation and Returning evidence.
iii. Brian Carrier and Eugene Spafford (Carrier & Spafford 2003) proposed The Integrated Digital Investigation Model that organizes the process into five groups consisting all in all 17 phases: Readiness phases, Deployment phases, Physical Crime Scene Investigation phases, Digital Crime Scene Investigation phases, and Review phase techniques to constitute a proactive way for handling cyber crime incidents.
iv. A Hierarchical, Objectives-Based Framework for the Digital Investigations Process (Beebe & Clarke 2004) is another model that proposed a multi-layer, Hierarchical frame work to guide investigators. It has six phases which are: Preparation, Incident Response, Data Collection, Data Analysis, Findings Presentation and Incident Closure.

The Model Phases Overview

Phase 1: Preparation

As the name implies, it's the preparatory stage of the investigation where all logistics are listed, examined and evaluated to attest its capability, efficiency and compatibility to handle the investigation at hand. This phase is subdivided into: Pre-preparation, Case evaluation, Preparation of detailed design for the case, Preparation of investigation plan and Determination of required resources.

Phase 2: Physical Forensics and Investigation

The collection, preserving, analyzing the physical evidences and the reconstruction of what transpired at the crime scene, is the sole purpose of this stage or phase. Hence this phase is further subdivided into Physical preservation, Preliminary survey on physical scene, Evaluate the physical scene, Initial documentation, photographing and narration, Search and collection of physical evidence and Final survey for physical crime scene.

Phase 3: Digital Forensics

This phase starts according to the case, as in network attacks it works in parallel with the physical forensics and investigation phase, while in other attacks it can start after it is done. The goal of this phase is to identify and collect the electronic events that occurred on the system and analyze it, so that it can be used with the results of the previous phase to reconstruct events.

Digital forensics phase includes sub phases which are Evaluation and Assessment, Acquisition of digital evidences, Survey the digital scene, Digital Evidence Examination, Reconstruction of extracted data and Conclusion.

Phase 4: Reporting and Presentation

After the above phases are collectively and perfectly executed, the reporting and presentation phase can thence be applied according to the constitutional rights binding such crime in the country of operation as this phase presents the conclusions and corresponding evidence from the investigation.

In a corporate investigation, the audience typically includes the general counsel, human resources, and executives. Privacy laws and corporate policies dictate what is presented. In a legal setting, the audience is typically a judge and jury, but lawyers must first evaluate the evidence before it is entered (Carrier 2002).

Phase 5: Closure

This phase is termed the final stage of the digital forensic investigation where the review of all the above process is carried out and then to examining how well each of the physical and digital investigations worked together, and whether the evidences collected were enough to solve the case, and ensures returning of the physical and digital properties back to its owner.

Model Discussion and Conclusion

With high increase rate of cyber crime in the society or the nation at large, and how sophisticated these miscreants are becoming, there should be also a high need for expertise in the field of digital forensic investigation with purposeful guidance for these experts to perform the investigation without altering the integrity of evidences.

The model discussed in this study is a suggestive and a detailed step by step model which when adopted with more reviews, it will serve efficiently in digital forensic investigation.

As digital forensic is a system base application, the need for user friendly operating systems is necessary. Hence, user friendly operating system such as windows, UNIX and Linux are recommended. The model suggested in this study allows technical requirements for each phase to be developed and identifies interaction between physical and digital investigations. This

technically designed model can be used by law enforcement agencies as well as corporate scenarios.

In conclusion to the above study, digital forensic provides digital evidence which is normally challenged in court in the proceed of any related case, therefore the use of standard procedures and models increases the chances of the courts' acceptance of such cases, also the inclusion of commonly used procedures from physical forensics will be a plus to the credibility of the analyzed results from the digital world.

Recommendation for Policy and Practices

Digital forensic is a technical procedure if well implemented, it will enhance the administration of justice base on the verified evidences gotten from digital forensic investigation. Therefore there is a need to include digital forensic into existing laws to be implemented in the existing policies, technical and legal requirements for evidence admissibility.

Also there is a need for a standard procedure that is streamlined to ensure harmony between lawyers, judges, forensic experts, law enforcement agencies, corporations, individuals, and the court must be adhered to.

There should also be a sensitization on digital forensic by educating the general populace on its effective and efficient results in providing investigative evidences with proofs, thereby eliminating the traditional way of investigation which is stressful and time wasting.

REFERENCES

Asian School of Cyber Laws (2006), 'Asian School of Cyber Laws', www.asianlaws.org, 12/2006.

Association of Chief Police Officers (2005), 'Good Practice Guide for Computer based Electronic Evidence', available at: http://www.nhtcu.org.

Antwi-boasiako, A., Venter, H., Antwi-boasiako, A., Venter, H., Model, A.,Evidence, D., & Assessment, A. (2018). A Model for Digital Evidence Admissibility Assessment To cite this version : HAL Id : hal-01716394.

Apau, R., & Koranteng, F. N. (2020). Forensic Science International : Synergy An overview of the digital forensic investigation infrastructure of Ghana. Forensic Science International: Synergy, 2, 299–309. https://doi.org/10.1016/j.fsisyn.2020.10.002

Ay, O., & Akoto, D. (2020). Digital Forensics Investigation Jurisprudence : Issues of Admissibility of Digital Evidence. https://doi.org/10.24966/FLIS- 733X/100045

Baryamureeba Venansius and Tushabe Florence (2004), 'The enhanced digital process model', Institute of Computer Science, Makerere University, www.makerere.ac.ug/ics.

International, K. (n.d.). Cross-border investigations: Are you prepared for the challenge?

Joseph, A. (2018). Digital Forensics in Distributed Environment. April. https://doi.org/10.4018/978-1-5225-4100-4.ch013

Kao, D. (2016). Cybercrime investigation countermeasure using created- accessed modified model in cloud computing environments. September 2015.

Khanafseh, M., & Qatawneh, M. (2019). A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics. September. https://doi.org/10.14569/IJACSA.2019.0100880

Mahfouz, M., & Adjei-quaye, A. (2017). Computer & Cyber Forensics: A Case Study of Ghana Computer & Cyber Forensics: A Case Study of Ghana. January.

Patil, R. Y., & Devane, S. R. (2022). Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime. Journal of King Saud University – Computer and Information Sciences, 34(5), 2031–2044.

https://doi.org/10.1016/j.jksuci.2019.11.016

Practices, S. B., & Acquisitions, C. F. (2018). Scientific Working Group on Digital Evidence Scientific Working Group on Digital Evidence. 0, 1–11.

Ryan, D. J. (n.d.). Legal Aspects of Digital Forensics.

Sriram Raghavan. (n.d.). Digital forensic research: current state of the art.

Standard, T., & Last, W. A. S. (2018). THIS VERSION REMAINS CURRENT.