TEN

LEGAL ISSUES AND CHALLENGES IN THE ADMISSIBILITY OF DIGITAL FORENSIC EVIDENCE IN COURTS IN NIGERIA

by

G.V. OBAMANU1*

Abstract

In Nigeria, the admissibility of digital forensic evidence in court proceedings poses significant challenges and raises important legal issues. This paper aims to analyze the current state of admissibility rules and practices in Nigerian courts regarding digital forensic evidence and highlight the associated challenges. The study will delve into the provisions of the Nigerian Evidence Act, particularly Section 84, which addresses the admissibility of computer-generated evidence. By examining whether these provisions adequately cover digital forensic evidence, this paper will determine the applicability of existing laws in the Nigerian legal system. Through a comprehensive review of relevant legislation, case law, and judicial precedents, this paper will address the gaps and limitations in the current legal framework. It will identify any ambiguities or inconsistencies in the admissibility criteria for digital forensic evidence, which may hinder its effective utilization in court. The paper methodology will involve a thorough examination and analysis of relevant legal documents, including the Nigerian Evidence Act, relevant case studies, and scholarly literature. Comparative analysis with international practices and experiences, particularly from jurisdictions such as the United States, the United Kingdom, and Australia, will be considered to provide broader insights. The findings of this paper will highlight the current landscape of admissibility regulations in Nigerian courts and shed light on the legal issues and challenges surrounding digital forensic evidence. Moreover, the study will propose recommendations to address any gaps or limitations identified, aiming to improve the legal framework and enhance the admissibility of digital forensic evidence in Nigerian courts.

Introduction

In today's digital age, the increasing reliance on technology and interconnected systems has resulted in a heightened vulnerability to cyber threats and crimes. The constant evolution of cyber threats necessitates a robust system for ensuring cyber security, which involves the effective utilization of digital forensic evidence. Safeguarding digital infrastructures and information is crucial for protecting national security, economic stability, and citizens' privacy. Nigeria, as Africa's largest economy and a hub for digital innovation, is susceptible to significant risks such as hacking, identity theft, data breaches, ransomware attacks, and financial fraud. While Nigeria's digital transformation has presented opportunities for

economic growth and societal advancement, it has also attracted cyber criminals who exploit system vulnerabilities and target unsuspecting individuals and organizations. In response to the growing cyber threat, the Nigerian government enacted the Cybercrime (Prohibition, Prevention, Etc.) Act in 2015 to criminalize various cyber activities and provide legal means to combat cybercrimes. However, challenges arise when it comes to the admissibility of digital evidence in court proceedings since the Evidence Law regime in Nigeria has yet to make provisions for the admissibility of digital forensics evidence. This reliance on the admissibility of computer-generated evidence can eventually lead to inconsistencies in judicial decisions and subsequent difficulties in prosecuting cyber criminals. Therefore, to ensure the success of cybercrime investigations, digital forensic evidence needs to meet admissibility requirements, including demonstrating authenticity, reliability, integrity, and relevance in a court of law. However, several factors impede the seamless integration of digital forensic evidence into the Nigerian legal system.

History of Digital Cyber Security in Nigeria

Cyber security in Nigeria has witnessed significant developments over the years as the country has grappled with the ever-growing threat of cybercrime2[1]. In the early days of Internet adoption in Nigeria, cyber security was not a major concern. However, with the increasing use of technology and the Internet for various activities, such as e-commerce, online banking, and communication, the country began to face escalating cyber threats.

One of the early milestones in Nigeria's cyber security journey was the establishment of the Nigerian Communications Commission (NCC) in 1992. The NCC played a crucial role in regulating and overseeing the telecommunications industry, including issues related to cyber security. It worked towards creating a safe and secure digital environment for Nigerians. In 2001, the Nigerian government developed the National Information Technology Development Agency (NITDA) to focus on the development and regulation of information technology in the country[2]. NITDA has since been actively involved in fostering cyber security awareness, promoting best practices, and implementing policies to strengthen the country's cyber security framework. As the threat landscape evolved, Nigerian organizations and individuals faced numerous cyber-attacks, such as phishing, hacking, and online scams. These attacks not only affected individuals but also had significant implications for national security, financial systems, and critical infrastructure. To address these challenges, the Nigerian government increased its focus on cyber security measures. In 2014, the Cybercrime Act was enacted, which provided a legal framework for combating cybercrime in the country.

This legislation criminalized various cyber activities, such as unauthorized access to computer systems, cyber stalking, and identity theft, and outlined penalties for offenders. In recent years, the Nigerian government has taken steps to enhance collaboration between relevant agencies and public-private partnerships to strengthen cyber security[3]. The establishment of the National Cybersecurity Policy and Strategy (NCPS) in 2014 aimed to create a framework for the protection of critical national information infrastructure and the promotion of cyber security awareness. Furthermore, Nigeria has participated in regional and international initiatives to combat cyber threats. The country is a member of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and has participated in regional exercises and capacity-building workshops related to cyber security[4]. Despite these efforts, Nigeria continues to face challenges in cyber security, including limited awareness, skills gaps, inadequate infrastructure, and funding constraints. However, the government and relevant stakeholders are continuously working towards strengthening the country's cyber security capabilities. Nigeria's journey in cyber security has evolved over time, reflecting the increasing importance of addressing cyber threats. The government and relevant agencies have taken steps to enhance awareness, develop policies, enact legislation, and foster collaboration to mitigate cyber risks[5]. However, ongoing efforts are necessary to address the evolving nature of cyber threats and ensure a secure digital environment for Nigerians.

Categories of Cyber Crimes

Cybercrime has become a significant concern worldwide, and Nigeria, like many other countries, faces various challenges in combating this menace. With the rapid growth of technology and digitalization,

---

* L.L.B (Hons), B.L., LL.M., FCIHRM., CFC., CFI

[1]Oke, R., 'Cyber Capacity without Cyber Security: A Case Study of Nigeria's National Policy for Information Technology (NPFIT)' (2012) vol 12 The Journal of Philosophy, Science and Law'

[2]E Edeaghe and T Okurumeh, "Digital Forensic as a Tool for Fighting Cyber Crime in Nigeria" (2015) 5(6) Forensic Paper and Technology, 28-39

[3](n 2) 28-39

[4]E Enejeta, Cyber security threats heighten in financial sector. (2016) Availablehttp://www.financialwatchngr.com/2016/05/27/cyber-security-threats-heighten-financial-sector/ Accessed 20th July, 2023.

[5]L Babajide, Nigeria ranked third in the world for cybercrime. (2026) Available at:http://crimeworldnaija.blogspot.com.ng/2016/07/nigeria-ranked-third-in-world-for-cyber.html Accessed 20th July, 2023.

the country is witnessing a surge in cybercriminal activities. The following are some of the cybercrimes prevalent in Nigeria.

1. **Hacking and Unauthorized Access:** One of the most common forms of cybercrime in Nigeria is hacking and unauthorized access. Cybercriminals use sophisticated techniques to breach computer systems, networks, and databases unlawfully[6]. They gain unauthorized access to sensitive information, financial data, personal information, and government databases. Such criminal activities can lead to identity theft, financial losses, and national security breaches.

2. **Phishing and Social Engineering:** Phishing is a technique used by cybercriminals to deceive individuals and acquire personal and financial information[7]. This typically involves sending fraudulent emails, text messages, or creating fake websites that appear trustworthy. Once victims disclose their sensitive information, it is misused for financial fraud, identity theft, or unauthorized access to their accounts. Social engineering involves manipulating individuals to gain confidential information or unauthorized system access through psychological manipulation.

3. **Online Fraud:** Online fraud encompasses various activities aimed at defrauding individuals or organizations[8]. This includes advanced fee fraud (419 scams), lottery scams, investment scams, and romance scams. Cybercriminals deceive victims into sending money or providing personal information with the promise of financial gain or rewards. These fraudulent activities result in substantial financial losses and emotional distress.

4. **Identity Theft:** Identity theft is a severe crime where criminals steal and impersonate someone's identity for personal gain. They acquire personal data through hacking, phishing, or other means, then use it to open fraudulent bank accounts, apply for loans, make unauthorized purchases, or commit other criminal acts. Identity theft not only causes financial damages but also ruins victims' reputations and affects their lives significantly.

5. **Cyberbullying and Online Harassment:** The emergence of social media platforms has given rise to cyberbullying and online harassment[9]. In this category of cybercrime, individuals use digital platforms to harass, threaten, defame, or intimidate others. Cyberbullying has adverse psychological effects on victims, particularly children and teenagers. It can lead to social isolation, depression, and sometimes even self-harm or suicide.

6. **Cyber Terrorism:** Cyber terrorism involves the use of technology to carry out political, ideological, or religious motives to cause harm or disruption[10]. This includes hacking into government websites, disrupting critical infrastructure, spreading propaganda, or conducting cyber-attacks that jeopardize national security.

Overview of Digital Forensic Evidence in Nigeria

The emergence of information technology has ushered humanity into an era of high-tech communication and digital platforms, revolutionizing the transfer of information, transactions, and automation. This technological advancement has significantly transformed human activities and consequently reshaped the landscape of legal proceedings in courts worldwide. To keep up with these modern developments, it is crucial for the law to adapt accordingly[11]. In Nigeria, the use of computers and electronic storage

---

[6] F.E. Eboibi, "Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence" (2010) 10 Nigerian Law and Practice Journal, 139-160

[7] *Ibid*

[8] *Ibid*

[9] Kehinde Adegbite, Law and Forensic: Techniques of Evidence Gathering and Case Presentation in Court, 11 October 2014, available at http://www.nigeriavillagesquare.com/articles/law-and-forensic-techniques-of evidence-gathering-and-case-presentation-in-court.html Last accessed 4th July 2023

[10] *Ibid*

[11] P.A Akhihiero, "Admissibility of Electronic Evidence in Criminal Trials, How Practicable"? Being a paper presented at the 2013 Annual General Meeting of the Magistrates Association of Nigeria, Edo State, from 23rd of July, 2013

and communication systems has experienced a sharp increase in commercial and financial transactions[12]. As a result, the utilization of digital evidence has become more prevalent. Courts now accept various forms of digital evidence, including emails, digital photographs, ATM transaction logs, word processing documents, instant message histories, accounting program files, internet browser histories, databases, computer memory contents, backups, computer printouts, Global Positioning System (GPS) tracks, logs from electronic door locks, and digital video or audio files[13]. Digital evidence has thus assumed a crucial role in the adjudication of both criminal and civil cases.

In Nigeria, the law of evidence, specifically Section 84 of the Evidence Act 2011, has established provisions for the admissibility of computer-generated or electronic evidence. This provision ensures that the court can assess and consider digital evidence in legal proceedings. Forensic science, encompassing various evidence-related disciplines, plays a pivotal role in court proceedings. Some forensic disciplines are laboratory-based, such as nuclear and mitochondrial DNA analysis, toxicology, and drug analysis. Others involve the interpretation of observed items, like fingerprints, writing samples, tool marks, bite marks, and species identification. Additionally, certain forensic disciplines combine experiential and scientific knowledge, such as explosives and fire debris analysis, as well as blood spatter analysis[14].

In a court of law, the judge ultimately determines which facts establish specific consequences. Consequently, forensic evidence can only be viewed as opinion evidence, though it may be referred to as such in a condescending manner[15]. Opinion evidence involves drawing conclusions and inferences from observable and communicable data or facts. It can be presented through oral testimony or in written reports. However, the evidential value of oral testimony can be affected by various considerations, just as submitting a written report without proper context may carry little weight[16]. As a general rule, opinion evidence is inadmissible, and witnesses may only speak to facts that they personally perceived, not the inferences drawn from those facts. However, there are exceptions to this general rule, outlined in sections 68 to 76 of the Evidence Act. For example, an appropriately qualified expert can provide an opinion on a matter that requires specialized expertise, while a non-expert witness can provide an opinion on a matter not demanding particular expertise but serves as a means of conveying personally perceived facts. Forensic evidence predominantly falls within the realm of expert opinion, and our discussion centers on this aspect. Nonetheless, the court should consider whether the witness is better positioned than the court to form an opinion or draw inferences from the facts. It is essential to note that the common law prohibits opinion evidence from being given about a fact in issue, as that is solely the domain of the judge.[17] Despite the introduction of forensic evidence to aid crime detection and enhance the judicial process, there are still challenges to overcome in Nigeria. One major issue is the lack of adequate funding for the police and judiciary, hindering the conduct of thorough forensic investigations[18]. Additionally, there may be limitations in the availability of trained forensic experts and resources.

In conclusion, digital forensic evidence has become increasingly significant in Nigeria's legal system, with the use of computers and electronic communication systems on the rise. The admissibility of

---

[12] *Ibid*

[13] A Muzaffar, "The Admissibility of Modern Electronically Evidence in Criminal Cases under Islamic Law" Public Lecture Series , delivered at Faculty of Sharia & Law, Slains Islam University, Malaysia (USIM) 2013 Meaning of E-mail https://en.wikipedia.org/wiki/Message_transfer_agent Accessed 14th July, 2023.

[14] *Ibid*

[15] O. Maitama and others, "Cyber Crimes and Cyber Laws in Nigeria" (2013) 2(4) The International Journal of Engineering and Science, 121-156

[16] Ibid

[17] S.A Muzaffar, "The Admissibility of Modern Electronically Evidence in Criminal Cases under Islamic Law" Public Lecture Series , delivered at Faculty of Sharia & Law, Slains Islam University, Malaysia (USIM) 2013 Meaning of E-mail https://en.wikipedia.org/wiki/Message_transfer_agent Accessed 14th July, 2023.

[18] ` E Adomi, 'Combating Cybercrime in Nigeria'(2018) 26(5), The Electronic Library

computer-generated or electronic evidence is provided for under the Nigerian law of evidence. Forensic science plays a crucial role in court proceedings, but its evidence is considered opinion evidence subject to specific rules and exceptions. Challenges related to funding and resources need to be addressed to ensure the effectiveness of forensic investigations in Nigeria.

Types of Digital Forensic Evidence

Digital forensic evidence can take various forms and plays a critical role in investigations and legal proceedings. Here are some detailed explanations of the types of digital forensic evidence:

Computer

A computer is an electronic device that can perform various tasks, store and process information, and communicate with other devices or networks[19]. It consists of both hardware and software components that work together to provide functionality.[20] Computers are capable of executing complex calculations, running software applications, and storing vast amounts of data. They provide users with the ability to access information, communicate with others, and perform a wide range of tasks. A computer's hardware typically includes components like the central processing unit (CPU), memory, storage devices, input/output devices (keyboard, mouse, display), and connectivity options (wired or wireless).[21] A computer, in the context of digital forensics, can be an invaluable source of evidence in investigations related to cybercrimes, data breaches, intellectual property theft, fraud, and other digital offenses. The digital traces left behind on a computer can provide vital insights into the activities and intentions of individuals involved in such cases. When a computer is seized as part of a forensic investigation, forensic experts employ various techniques to examine and extract relevant data from its storage devices[22]. This process involves creating a forensic image, an exact replica of the original storage media, to preserve the integrity of the evidence. The forensic image is then analyzed using specialized software and tools[23]. The examination of a computer as forensic evidence can provide valuable information such as: Digital artifacts, Deleted files and metadata, Internet and network activity, User accounts and authentication, Malware and hacking tools and Communication and social media data. Investigating a computer as forensic evidence requires specialized knowledge and expertise to ensure the accuracy and integrity of the findings. Digital forensic experts follow strict methodologies and guidelines to collect, analyze, and present the evidence in a legally admissible manner.

Mobile Devices/Cellphones

Mobile devices/ cellphones forensics is a type of digital forensics that focuses on the investigation and analysis of mobile phones and other mobile devices as a source of valuable evidence[24]. With the increasing ubiquity of mobile phones and their significance in our daily lives, they have become a common presence at crime scenes, making them a crucial element to consider in forensic investigations. The main goal of mobile forensics is to extract and analyze data from mobile devices that can provide valuable insights into criminal activities, communication patterns, timelines, and connections between individuals. This can include retrieving call logs, text messages, multimedia messages (MMS/SMS), images, videos, audio recordings, chat conversations, contacts stored in the SIM card, and documents stored on the device[25]. Mobile forensics also encompasses the collection of network information, such as Wi-Fi networks and Bluetooth connections, which can be essential for determining the location of a device at a specific time or identifying potential co-conspirators[26]. Forensic experts specializing in

---

[19]M. Rouse, What does Computer Mean, available athttps://www.techopedia.com//definition/4607/computer#:. Accessed on 10th August, 2023

[20]Ibid

[21](n 19)

[22]I Darshan, 'Role of Computers in Digital Forensics' (2020) 6(7) IJSART, 2395-1052

[23]*Ibid*

[24]S. Perumal, 'Digital Forensic Model Based on Investigation Process (2018) 9(8) International Journal of Computer Science and Network Security, 38-44.

[25] (n 24) 38-44.

[26]*Ibid*

mobile forensics employ specialized tools and software to acquire data from mobile devices. Depending on the device's make, model, and operating system, different techniques may be required to bypass security measures and gain access to the device's content.[27]

The analysis of mobile device data involves examining metadata, system logs, and the various databases and file systems used by the device. This analysis helps in establishing timelines, identifying relevant communication patterns, identifying deleted or hidden information, and potentially uncovering methods used to conceal evidence. Mobile forensics is essential in a wide range of criminal investigations, including cybercrime, fraud, theft, terrorism, and even cases of domestic or workplace disputes. It provides valuable evidence that can be presented in court to support and strengthen the prosecution's case.

File and Email Forensics

Emails are a common form of digital evidence in both criminal and civil cases. They can provide crucial information such as communications, timestamps, and attachments, which can establish the intent, motive, or involvement of the parties involved in a case[28]. Emails and file forensics also play a significant role in digital investigations. Files stored on devices or sent through various platforms can contain valuable evidence such as documents, images, videos, or even hidden data[29]. By analyzing these files, digital forensic experts can uncover important details related to a case, including file metadata, origin, modification dates, and user activities. This information helps investigators reconstruct events, identify culprits, verify authenticity, and ultimately strengthen the overall case.

Network Forensics

Network forensics involves the investigation and analysis of network activity and communication in digital investigations[30]. It focuses on examining network traffic, logs, and metadata to identify and reconstruct events, detect intrusions, analyze patterns, and gather evidence. Network forensics can provide crucial digital forensic evidence in various cases, including cyberattacks, data breaches, intellectual property theft, fraud, and other network-based crimes[31]. By analyzing network traffic, investigators can uncover information such as IP addresses, communication protocols, timestamps, session data, and data transfers. This evidence can help identify attackers, determine the extent of a breach, understand the methodology used, and track their movements within the network[32]. Generally, network forensics plays a vital role in digital investigations, providing valuable evidence that can be used in legal proceedings to establish the facts, attribute responsibility, and support or refute allegations.

Memory Forensics

Memory forensics is a branch of digital forensics that focuses on the analysis and extraction of data from a computer's volatile memory (RAM). It involves capturing a memory dump, which is a snapshot of the computer's active processes, running applications, and data in memory at a particular point in time. Memory forensics enables investigators to uncover valuable information that may not be readily available through traditional forensic methods.[33] This includes details such as open network connections, active processes, login credentials, encryption keys, malware artifacts, and evidence of suspicious or malicious activities. By analyzing the memory dump, forensic experts can reconstruct a timeline of events, identify running processes or hidden malware, recover encryption keys for further analysis, and identify any modifications or tampering that may have occurred during an incident.

---

[27] *Ibid*

[28] B Colin, 'The Future of Cyberterrorism, Crime and Justice International' (1997) 13(2) International Journal of Forensic, 15-18.

[29] *Ibid*

[30] I Darshan, 'Role of Computers in Digital Forensics' (2020) 6(7) IJSART, 2395-1052

[31] *Ibid*

[32] *Ibid*

[33] B. Carrier, 'Defining Digital Forensic Examination and Analysis Tools using Abstraction Layers' (2016) 1(4) International Journal of Digital Evidence, 1-12

Memory forensics is particularly useful in cases involving advanced persistent threats, memory-resident malware, rootkits, and other forms of stealthy or memory-based attacks.

Desk Imaging and Analysis

Desk imaging and analysis is a process used in digital forensics to capture and analyze the contents of a computer's hard drive or storage device. It involves creating an exact replica or image of the entire disk, including all data, files, partitions, and system information. The imaging process ensures that the original data is preserved and protected, as any changes made during analysis could compromise the integrity of the evidence[34]. It allows forensic investigators to work on a copy of the data without altering the original. Once the disk image is created, forensic analysts can use specialized software to conduct in-depth analysis. They examine file metadata, hidden or deleted files, system logs, and other artifacts to uncover evidence relevant to an investigation. This analysis can reveal information such as file access times, user activity, internet browsing history, document creation or modification dates, and more[35]. Desk imaging and analysis plays a crucial role in investigations related to computer crimes, data breaches, intellectual property theft, and other digital offenses. It allows forensic experts to reconstruct events, identify potential suspects, establish timelines, and gather evidence that can be presented in court.

Malware Forensics Analysis

Malware forensic analysis is a branch of digital forensics that focuses on the investigation and analysis of malicious software, or malware. This process involves analyzing the behavior, characteristics, and impact of malware to understand its origins, purpose, and potential impact on a system or network. To conduct malware forensic analysis, forensic analysts use specialized tools and techniques to acquire and examine malware samples, including viruses, worms, trojans, ransomware, and other types of malicious code[36]. The goal is to gather evidence and extract information that can help identify the malware's source, functionality, and potential damage. The process of malware forensic analysis typically involves several steps: Malware acquisition, Static analysis, Dynamic analysis, Reverse engineering, Malware categorization and documentation.

Admissibility of Electronic Evidence

Electronic evidence refers to evidence that is generated through mechanical or electronic processes[37]. It involves the use of electronically controlled machines or equipment, such as computers, satellite waves, cables, and communication systems, to gather evidence for use in a court of law. This type of evidence can be obtained from various sources, including emails, phone logs, ATM and POS transaction logs, social media records (e.g., Facebook, Twitter, WhatsApp, Instagram), videos on platforms like YouTube, and digital content stored in DVDs, CDs, and flash drives[38]. In the case of *Orogun & Anor v. Fidelity Bank*[39]the Supreme Court addressed the admissibility of electronically generated evidence, specifically pertaining to a GSM gadget and the information stored within it.

The court referenced Section 258 (1)(d) of the Evidence Act, which defines a document to include any device used for storing, recording, or retrieving information, including computer output. This provision broadens the definition of a document beyond traditional paper-based records, recognizing the significance of electronically generated evidence in modern times. In the case at hand, a GSM gadget was submitted as evidence, along with the message or information stored within it. The court held that since the GSM gadget falls within the definition of a document under Section 258(1)(d), it can be

---

[34]C Gupta, 'Systematic Digital Forensic Investigation Model' (2017) 5(1) International Journal of Computer Science and Security, 118-131

[35]*Ibid*

[36]M. D.Kohn and others, 'Integrated Digital Forensic Process model' (2016) 38 Computers & Security, 103 - 115. (2016).

[37]P A Anyede, 'Appraisal of Admissibility of Electronic Evidence in Legal Proceedings in Nigeria' (2019) 29 Journal of Law, Policy and Globalization, 3

[38]*Ibid*

[39](2018) LPELR-46601(CA),

tendered in evidence. Once admitted, the information stored within the GSM gadget is also considered documentary evidence.

The admissibility of electronic evidence is unique and separate from the conditions for admitting evidence in civil and criminal trials. Therefore, when determining the admissibility of electronic evidence, the court must consider the provisions stated in section 84 of the Act. This means that computer-generated documents or documents downloaded from the internet are subject to the conditions outlined in section 84 of the Evidence Act, 2011. Section 84 specifically provides guidelines for the admissibility of electronically generated evidence. It states that a statement contained in a document produced by a computer can be admitted as evidence if certain conditions are met. These conditions include the document being produced by the computer during a period in which it was regularly used to store or process information, and that the computer was operating properly and receiving relevant information during that period. Additionally, if multiple computers were involved in storing or processing information during that period, they are considered as one computer for the purposes of admissibility.

Additionally, section 84 requires the party seeking to tender a computer-generated statement or document to file an authentication certificate. This certificate must identify the document or statement, describe the manner of its production, state the particulars of the device used, and be signed by a person in a responsible position in relation to the operation of the device or the management of the activities. The authentication certificate is a legal requirement aimed at ensuring the authenticity of electronic evidence before it can be admitted. Failure to comply with this requirement renders the evidence inadmissible. The provision in section 84 regarding the authentication certificate was adopted from the English Police and Criminal Evidence Act. It allows for the certificate to be signed by a person who does not necessarily have to be an expert, as long as they can provide proof of the computer's reliability. It is important to note that the conditions stipulated in section 84 for the admissibility of electronic evidence are mandatory, and failure to properly lay them before the court will result in the rejection of such evidence. To lay a proper foundation for electronically generated evidence, it is necessary to establish its relevance to the case and authenticate the reliability of the computer that produced it. Under Nigerian law, there are four evidence standards that electronic documents must satisfy to be admissible in evidence. These include being pleaded, relevant to the fact in issue, admissible in law, and satisfying the requirements of authentication as outlined in section 84 of the Evidence Act, 2011[40].

Furthermore, it is important to note that the admissibility of electronically generated documents in court requires more than just their tendering. In the case of *Sylva & Anor v INEC & Ors*[41] the Court clarified that once an electronically generated document is admitted as evidence, it must be demonstrated or played to prove the alleged facts. In other words, the document cannot simply remain a closed or 'sleeping' document, serving no purpose other than cluttering the court proceedings. If the document is not properly presented or played to establish the facts it claims to prove, it becomes unusable and should not have been brought before the court in the first place. Thus, it is crucial to fulfill all necessary pre-conditions and ensure the effective presentation of electronically generated evidence to ensure its admissibility and relevance in legal proceedings.

Admissibility of Digital Forensics Evidence as Electronic Evidence

The admissibility of digital forensics evidence as electronic evidence has been addressed by provisions of the Evidence Act 2011 in Nigeria[42]. The provision of Section 67 of the Evidence Act 2011 negated the application of opinion evidence when it stated thus: 'The opinion of any person as to the existence or non-existence of a fact in issue or relevant to the fact in issue is inadmissible except provided in ss. 68 to 76 of this Act.' The basis for this exclusion is that opinion is a conclusion; hence, it is often irrelevant, unreliable, and logically worthless, and it tends to usurp the functions of the courts whose

[4041] Ayodeji v FRN (2018) 45839 (CA)

[41] (2016) LPELR-45730 (CA)

[42] F.E. Eboibi, 'Cybercrime Prosecution and The Nigerian Evidence Act, 2011: Challenges of Electronic Evidence' (2011) 10 Nigerian Law and Practice Journal, 139-160

exclusive duty is to draw conclusions and inferences from the available evidence.[43] However, the opinion of a digital forensic expert who appears in court to give digital forensic evidence is not regarded as an opinion by virtue of section 68 of the Nigerian Evidence Act 2011. Section 68 (1) provides that:

When the Court has to form an opinion on a point of law, customary law or custom, or of science or art, or as to identity of hand writing or conducting finger impressions, the opinions upon that point of persons especially skilled in such foreign law, customary law or custom, or science or art, or in questions as to identity of handwriting or finger impressions, are admissible.

Furthermore, section 68(2) of the Nigerian Evidence Act 2011 expressly states who an expert is when it provides that: 'Persons so especially skilled as mentioned in subsection (1) of this section are called experts.' The legal implication of section 68 is that digital forensic being 'the science of locating, extracting, and analyzing types of data from different devices, which specialists then interpret to serve as legal evidence" is acceptable in the Nigerian Courts and not regarded as opinion evidence. It means that digital forensic evidence emanating from handwriting, computer, DNA, mobile phone, fingerprints analysis sought to be presented in court by digital forensic experts are allowed. Although there is no specific legal framework on digital forensic in Nigeria, the practice of digital forensics has been given the force of law by section 68 of the Nigerian Evidence Act 2011. Moreover, section 258 of the Nigerian Evidence Act 2011 definition of documents to include electronic documents and devices and section 84(1) which provides for the admissibility of digital evidence as follow that:

> 'In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question'.

Also, the enactment of the Nigerian Cybercrimes Act 2015 also emphasizes the importance of digital forensic evidence. This act specifically addresses cybercrime offenses and recognizes that digital information is often essential in proving or disproving the guilt or innocence of a cybercrime perpetrator[44]. Therefore, digital forensic evidence is crucial in such cases and forms part of the overall evidence presented in court. Additionally, the Nigerian Administration of Criminal Justice Act 2015 further enhances the application of digital forensic evidence. This Act restricts the extraction of confessional statements from suspects by law enforcement agents. As a result, digital forensics investigations are necessary to identify and prosecute perpetrators of crimes in Nigeria. This highlights the importance of the expertise provided by digital forensic experts in recovering and presenting evidence in court.

In conclusion, the admissibility of digital forensic evidence as electronic evidence is supported by various provisions in the Nigerian Evidence Act, the Nigerian Cybercrimes Act, and the Nigerian Administration of Criminal Justice Act. Digital forensic evidence obtained from various sources, such as handwriting analysis, computer analysis, DNA analysis, mobile phone analysis, and fingerprint analysis, is considered acceptable in Nigerian courts. The recognition of digital forensic evidence reinforces the importance of the practice in the Nigerian legal system, ensuring that perpetrators of crimes can be properly identified and prosecuted.

Evidential Weight of Digital Forensics Evidence

In the realm of digital forensics as it is with electronic evidence, the admissibility of evidence plays a crucial role in legal proceedings. However, it is essential to underline that the admissibility of digital forensic or electronic evidence should not be confused with the weight and probative value assigned to it. This distinction is particularly important in Nigeria's legal system, as highlighted by the case of *Atuma*

[43] *Ibid*

[44] (n 43) 139-160

v. APC & Ors.[45] The admissibility of digital forensic evidence as it is with electronic evidence refers to its acceptance as part of the legal proceedings.

This determination is primarily based on whether the evidence has been obtained and presented following legally acceptable methods, such as adhering to established protocols under section 84 of the Evidence Act and ensuring the integrity and authenticity of the evidence[46]. Once the evidence satisfies these criteria particularly the conditions set out in section 84(2) of the Act, it becomes admissible and can be considered by the court. While the admissibility allows the evidence to be considered by the court, it does not automatically dictate the weight or probative value attributed to it. The weight of digital forensic evidence relates to its strength and significance in supporting or refuting a party's claims. The probative value of the evidence signifies its ability to prove or disprove relevant facts in the case.

In the case of *Atuma v. APC & Ors* supra, the court elucidated that the admissibility of evidence is distinct from its weight or probative value. Merely being admitted in court does not guarantee that the digital forensic evidence will carry substantial weight. The court will assess the evidence based on its credibility, reliability, and persuasiveness, considering the specific facts and circumstances of the case. Determining the weight and probative value of digital forensic evidence involves analyzing various factors. These may include the qualifications and expertise of the digital forensic examiner, the integrity and reliability of the methods used to collect and analyze the evidence, and the consistency and coherence of the findings with other pieces of evidence.

Conditions for the Admissibility of Digital Forensics Evidence

Having established the law that the Evidence Act allows for the admissibility of digital forensics evidence by virtue of the provisions of section 258 and 84(1) of the Evidence Act 2011, then the conditions for the admissibility of electronic evidence will apply. Section 84(1) provides as follows:

'In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question'.

As stated above, Section 84(1) states that in any legal proceeding, a statement contained in a document produced by a computer can be admitted as evidence if certain conditions are met. These conditions include:

(a) The document was produced by the computer during a period when it was regularly used to state or process information for activities regularly carried out,
(b) The computer regularly received information of the same kind as that contained in the statement,
(c) The computer was operating properly or any issues it had did not affect the production or accuracy of the document, and
(d) The information in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

If multiple computers were used over a period for storing or processing information, they are considered as a single computer for the purposes of this section. A certificate identifying the document and how it was produced, as well as providing details about any devices involved can be used as evidence. The certificate must be signed by a person in a responsible position related to the operation of the device or management of the activities.

Additionally, information is considered supplied to a computer if it is provided in an appropriate form, whether directly or through equipment. If information is supplied to a computer for storage or processing purposes outside of the activities in which it operates, it will still be considered supplied in the course

[45](2023) LPELR-60352(SC).
[4647]Ibe v A.G & C.J., Enugu State & Ors. (2023) LPELR-60305 (CA)

of those activities. Finally, a document is considered produced by a computer whether it was directly produced by the computer or with the assistance of equipment.

In the case of *Polaris Bank v Centre Point Travel Agency Ltd*[47], the court emphasized the conditions for the admissibility of computer-generated documents. The court stated that for a document generated through a computer to be legally admissible, it must comply with Section 84(2) and (4) of the Evidence Act. The court further explained that a witness who intends to tender and rely on electronically generated evidence must establish a proper foundation for its admissibility as prescribed under Section 84(2) and (4) of the Act. This means that the witness must satisfy the requirements set out in those sections in order for the electronic document to be considered admissible as evidence.

Therefore, in this case and in accordance with the law, any computer-generated document must meet the conditions outlined in Section 84(2) and (4) of the Evidence Act in order to be admissible in court. The court places importance on laying a proper foundation for the admissibility of electronic evidence, emphasizing the need for compliance with the prescribed statutory provisions.

Also, in the case of *Kubor & Anor v. Dickson & Ors*[48], the Supreme Court held that a party seeking to tender a computer-generated document as evidence must go beyond simply submitting the document to the court. They must also provide evidence relating to the use of the computer and establish the conditions outlined in Section 84(2) of the Evidence Act, 2011. The court emphasized that the certificate required by Section 84(2) of the Evidence Act must be presented alongside the computer-generated evidence. Failing to do so renders the document illegally admissible and it should be expunged from the record at the judgment stage. The court further noted that the fact that the document was admitted into evidence without objection is irrelevant, as the admissibility of computer-generated evidence depends on satisfying the requirements set out in the Evidence Act.

The Best Evidence Rule and Digital Forensics Evidence

The best evidence rule, a principle of originality, states that original copies of documents and eyewitness accounts are considered the most reliable evidence. According to this rule, only original documents are admissible, unless permitted by

law[49]. This rule is a fundamental principle in the development of evidence law. The study of evidence law has focused on determining what qualifies as the best evidence, what is relevant in proving or disproving disputed facts, and what evidence should be excluded for fairness and justice[50]. The best evidence rule originated in the 18th Century case of *Omychund v Barker*[51], where Lord Harwicke declared that only the best evidence allowed by the nature of the case should be admitted. The rule, in its basic form, excludes any evidence that is not considered the best. Two sections of the Evidence Act illustrate this principle: sections 126 and 37. Section 126 applies to oral evidence and states that it must be direct and provided by a witness who directly experienced the fact in question. For example, if the fact can be seen, the witness must have seen it; if it can be heard, the witness must have heard it. If the evidence pertains to an opinion, it must be provided by the person who holds that opinion and can explain the grounds for it.

[47](2022) LPELR-57359 (CA)

[48] (2012) LPELR-9817(SC)

[49]M.H Graham, 'The Original Writing (Best Evidence) Rule: A Primer' (2019) 55 CRIM.L.BULL, 441

[50]*Ibid*

[51](1745) 1 Atk, 49, 26 ER 15, 33

The term "digital evidence" refers to any form of evidence that exists in a digital format, such as emails, digital photographs, social media posts, or computer-generated documents[52]. Unlike traditional forms of evidence that are physical in nature, digital evidence is intangible and requires specific methods to access and present it in court. Until digital evidence is printed or otherwise transformed into a tangible format that can be physically shown to the court, it remains in its digital form[53]. This change in format, from digital to physical, has raised concerns about the qualification of electronic evidence under the best evidence rule. The best evidence rule is a legal principle that generally states that the original copies of documents and eyewitness accounts are considered superior forms of evidence. It posits that, except as allowed by law, only the original versions of documents should be admitted as evidence in court.[54] This rule developed as one of the major principles governing the law of evidence.

In the case of digital evidence, the question arises as to whether the best evidence rule can be successfully applied. There is debate as to whether electronic evidence and reliance on digital technology. The Evidence Act addresses this issue by regarding computer evidence as equivalent to original evidence, as long as the conditions outlined in Section 84 of the Act are met. Section 84 provides detailed provisions on how computer evidence should be collected, preserved, and presented in court. Admissibility of computer evidence is primarily determined by its relevance to the case at hand. It is important to note that while the best evidence rule traditionally emphasizes the importance of original physical evidence, the Evidence Act recognizes that digital evidence can be treated as original evidence if it meets the conditions set forth in Section 84. However, the unique nature of digital evidence and its reliance on technology necessitate careful consideration and adherence to the relevancy criteria in order to ensure its admissibility in court.

Rationale for Equating Digital Forensics Evidence with Original Evidence

The treatment of computer evidence as original evidence holds significant advantages for the legal process. In criminal cases, this approach allows the prosecution to present electronic evidence directly in court, offering a more effective means of proving the guilt of the accused compared to relying solely on traditional forms of evidence. For instance, forensic examinations and analysis, such as DNA testing, can help resolve criminal cases where physical evidence may be scarce or destroyed[55]. By admitting all forms of computer output as original evidence, the Evidence Act recognizes the potential for manipulation or tampering, and thus imposes conditions for authentication and proof of integrity to ensure the admissibility of electronic evidence. It is important to acknowledge that manipulating or falsifying electronic evidence is relatively easy for sophisticated cyber criminals, and as a result, electronic data and records are susceptible to alteration, corruption, or forgery. However, technological advancements have also provided solutions to address these challenges. The field of computer forensic analysis, for example, offers techniques and methodologies to investigate and retrieve electronic evidence in a manner that preserves its integrity and authenticity[56]. These practices involve employing specialized tools and procedures to extract and analyze data from digital devices, while following strict protocols to maintain the chain of custody[57].

---

[52]Digital Evidence and Forensics, available at https://nij.ojp.gov/digital-evidence-and-forensics Accessed on 25th August, 2023.

[53]D Mugisha, 'Digital Forensics: Digital Evidence In Judicial System' (2019) 10 International Journal of Cyber Criminology, 12

[54]*Ibid*

[55]H.J.P Akhihiero, Admissibility of Electronic Evidence in Criminal Trials. How Practicable? In: Being a paper presented at the 2013 Annual General Meeting of the Magistrates Association of Nigeria, Edo State, from 23rd of July, 129. https://www.nigerianlawguru.com/articles/practice%20and%20procedure/ADMISSIBILITY%20OF%20ELECTRONIC%20EVIDENCE%20IN%20CRIMINAL%20TRIALS.pdf. Accessed 25th August, 2023.

[56]European Judicial Network (2020) Transnational access to electronic evidence for criminal cases: trends and latest developments within the EU and beyond. https://www.ejn-crimjust.europa.eu/ejn/NewsDetail/EN/727. Accessed, 25th August, 2023.

[57]*Ibid*

By equating electronic evidence with original evidence, the legal system recognizes the transformative impact of technology in the modern world and acknowledges the need to adapt evidentiary rules accordingly. This approach allows for the admissibility of electronic evidence in its native digital format, eliminating the need for time-consuming and potentially unreliable conversions into traditional forms of evidence. Furthermore, by imposing authentication requirements, the legal system ensures that electronic evidence can withstand scrutiny and maintain its probative value in court proceedings.

Challenges of Admissibility of Digital Forensic Evidence in Nigerian Courts

The admissibility of digital forensic evidence in Nigeria faces several legal issues and challenges. These include:

1. **Lack of specific legislation:** One of the significant challenges is the absence of a specific legislation governing digital forensic evidence in Nigeria. There is a gap in the legal framework that addresses the admissibility and weight given to digital evidence in court proceedings. This creates uncertainty and inconsistency when admitting such evidence.

2. **Hearsay rule:** The hearsay rule poses a challenge to the admissibility of digital forensic evidence. According to the Nigerian Evidence Act, hearsay evidence is generally deemed inadmissible, unless it falls under specific exceptions. Digital forensic evidence, such as computer-generated records or data extracted from electronic devices, may fall under the hearsay category. Overcoming the hearsay rule becomes critical for the admissibility of digital forensic evidence.

3. **Authenticity and integrity:** Digital forensic evidence must prove its authenticity and integrity to be considered admissible. This requires demonstrating that the evidence was collected, preserved, and analyzed following established standards and protocols. Lack of proper documentation and handling practices can raise doubts regarding the authenticity and reliability of the evidence, making it challenging to gain acceptance in court.

4. **Expert testimony:** For the admissibility of digital forensic evidence, expert testimony plays a crucial role. The court needs to determine the competence, qualification, and credibility of the expert witness, as well as the methodology employed in obtaining and analyzing the evidence. The absence of specific guidelines to assess the competency and reliability of digital forensic experts can hinder the admissibility process.

5. **Privacy concerns:** Admitting digital forensic evidence may raise concerns about privacy and data protection. The extraction and analysis of digital evidence often involve accessing personal or confidential data. There is a need to strike a balance between the admissibility of evidence and protecting individuals' privacy rights, ensuring that the evidence obtained was legally and ethically acquired.

6. **Technical knowledge of the court:** Another challenge is the limited technical knowledge of the judiciary in digital forensic matters. Judges and legal professionals may struggle to fully comprehend the complexities and technical nuances associated with digital evidence. This lack of understanding can result in inadequate assessment and decision-making regarding the admissibility of digital forensic evidence. Addressing these legal issues and challenges requires the development of specific legislation on digital forensic evidence in Nigeria. It is essential to establish clear rules and guidelines that govern the admissibility, authenticity, and preservation of digital evidence. Additionally, training and capacity-building programs for judges and legal professionals can help enhance their technical understanding and competency in handling digital forensic evidence cases.

By addressing these issues, Nigeria can ensure the effective and reliable use of digital forensic evidence in its legal system, leading to improved cyber security and a more efficient justice system.

Conclusion

In conclusion, the paper conducted has shed light on the challenges faced in effectively utilizing digital forensic evidence in Nigeria for securing convictions and deterring cyber criminals. Despite the existence of legislation such as the Cybercrime (Prohibition, Prevention, etc.) Act of 2015, there are significant gaps and limitations in the admissibility of digital forensic evidence in the legal framework. The provisions of the Nigerian Evidence Act under Section 84, which address the admissibility of computer-generated evidence, do not specifically encompass digital forensic evidence. This lack of clarity raises concerns about the admissibility of such evidence in court proceedings, potentially hindering successful prosecutions of cyber offences. The absence of a standardized approach towards the admissibility of digital forensic evidence and varying levels of technical expertise within the legal system further complicate the situation. The lack of a clear and unified process for handling digital forensic evidence impedes efficient prosecution and leaves room for exploitation by cyber criminals, putting both individuals and critical infrastructure at risk.

Recommendations

1. **Update legislation:** The Nigerian Evidence Act should be revised to explicitly include provisions for the admissibility of digital forensic evidence. This will ensure that the legal framework keeps pace with technological advancements and addresses the specific requirements of digital investigations.

2. **Standardized approach:** A standardized approach should be developed for the admissibility of digital forensic evidence in Nigeria. This should include guidelines on the collection, preservation, analysis, and presentation of digital evidence to ensure consistency and reliability across different legal systems.

3. **Capacity building:** Efforts should be made to enhance the technical expertise of legal professionals, law enforcement agencies, and the judiciary in the field of digital forensics. Training programs and workshops should be conducted to improve their understanding of digital evidence and its admissibility in court.

4. **Collaboration between stakeholders:** Collaboration between the legal system, law enforcement agencies, and digital forensic experts is crucial. Regular meetings, knowledge sharing sessions, and partnerships should be fostered to ensure effective utilization of digital forensic evidence in court proceedings.

5. **Public awareness and education:** Public awareness campaigns should be conducted to educate individuals about the importance of digital forensic evidence in combating cybercrime. This will help in building public trust and support for the use of digital evidence in court.

6. **Paper and development:** Continuous paper and development in the field of digital forensics should be encouraged. This will facilitate the adoption of new technologies and methodologies, improving the quality and acceptance of digital forensic evidence in court.