THE ROLE OF DIGITAL EVIDENCE IN LEGAL PROCEEDINGS:

ADMISSIBILITY AND CREDIBILITY

BY

Precious OKPIMAH

LAW2002919

A LONG ESSAY WRITTEN AND SUBMITTED TO THE FACULTY OF LAW, UNIVERSITY OF BENIN IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF LAWS (LLB) OF THE UNIVERSITY OF BENIN, BENIN CITY.

DECEMBER, 2025

CERTIFICATION

I, **Precious OKPIMAH,** with Matriculation Number **Law2002919,** hereby certify that apart from references to other persons' work which have been duly acknowledged, the entire work is a product of my research, and this project has neither in whole nor in part been presented another degree elsewhere.

_____

Precious OKPIMAH

LAW2002919

APPROVAL

We certify that this project was written and completed by **Precious OKPIMAH**, with Matriculation Number **LAW2002919** in partial fulfilment of the requirements for the award of a Bachelor of Laws (LL.B) Degree.

DR. (MRS.) OBIAGELI FRANCISCA OSUJI _____

PROJECT SUPERVISOR **SIGNATURE AND DATE**

DR. (MRS.) OBIAGELI FRANCISCA OSUJI _____

PROJECT COORDINATOR **SIGNATURE AND DATE**

PROF. BRIGHT BAZUAYE

_____

DEAN, FACULTY OF LAW **SIGNATURE AND DATE**

DEDICATION

I dedicate this project to God Almighty for helping me this far, and to my dear family whom have been of great support to me, and to everyone who helped me in making this project successful.

ACKNOWLEDGEMENT

I would like to acknowledge some special persons dear to me, over the course of my stay in school and thank God for helping me.

First and foremost, I would like to thank God for helping me all through my stay in school, for strengthening me and encouraging me.

A big thanks to my supervisor, Dr (Mrs) Francisca Osuji, for her undeniable support and guidance in making this essay successful. To my lecturers and course mates, whom have impacted greatly in my life.

A special thanks to my parents for all the love and care, to my siblings Glory and Christabel for their love and encouragement.

To Uchechukwu Nicholas for his great support and courage.

To my dear friend Rebecca Nosa-Ojo for being a sister to me.

To Blessing Onize, a dear friend.

I am grateful to all. And a special thanks to myself for standing till the end.

TABLE OF STATUTES

Civil Evidence Act 1995 (UK)

Criminal of the Federal Republic of Nigeria 1999 (as amended)

Cybercrimes (Prohibition, Prevention, etc.) Act,2015 (as amended 2024)

Electronics Communication Act 2000 (UK)

Evidence Act 2011(as amended 2023)

Federal Rules of Civil Procedures (US,2006 amendments)

Federal Rules of Evidence (UK)

Police and Criminal Evidence Act 1984

Youth Justice and Criminal Evidence Act 1999 (UK)

TABLE OF CASES

LIST OF ABBREVIATIONS

CCE	-	Certified Computer Examiner
EIDAS	-	Electronic Identification, Authentication, and Trust Services
EnCE	-	EnCase Certified Examiner
EU's	-	European Union
GCFA	-	GIAC Certified Forensic Analysts
IOCE	-	International Organization on Computer Evidence
PACE	-	Police and Criminal Evidence
SWGDE	-	Scientific Working Group on Digital Evidence

TABLE OF CONTENTS

ABSTRACT

The digital revolution has fundamentally transformed the landscape of evidence in legal proceedings worldwide, with Nigeria taking a decisive step forward through the Evidence (Amendment) Act 2023. This research examines the evolving role of digital evidence in Nigerian courts, focusing on the critical issues of admissibility and credibility within the framework of the newly amended Evidence Act. The study addresses the transformative impact of sections 84A-84D, which revolutionized how electronic records, digital signatures, and computer-generated documents are treated in judicial proceedings. Prior to the 2023 amendments, Nigerian courts grappled with significant challenges in authenticating and admitting digital evidence under the restrictive provisions of Section 84 of the Evidence Act 2011. The landmark case of *Atiku Abubakar v. Muhammadu Buhari* exemplified these challenges, where the Supreme Court struggled with the admissibility of electronic voting records and server-generated data. This research investigates how the Evidence (Amendment) Act 2023 addresses these longstanding issues while establishing new standards for digital evidence credibility. The study employs doctrinal analysis, comparative jurisprudence, and empirical research methodologies to examine the practical implications of Nigeria's modernized digital evidence framework. Key findings reveal that while the 2023 amendments significantly enhance the admissibility of electronic records, challenges remain in ensuring credibility, particularly regarding authentication protocols and technical expertise requirements within the judiciary. This research contributes to legal scholarship by providing the first comprehensive analysis of Nigeria's reformed digital evidence regime, offering practical guidance for legal practitioners, and proposing recommendations for effective implementation of the new legislative framework.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The proliferation of digital technology in Nigeria has created an unprecedented volume of electronic evidence in legal proceedings, ranging from WhatsApp messages and email communications to blockchain transactions and artificial intelligence-generated content.[1] The Evidence Act 2011, particularly Section 84, proved inadequate in addressing the complexities of modern digital evidence, creating significant barriers to justice for ordinary Nigerians.[2]

The case of *Diamond Bank Plc v. Nwosu*[3] highlighted the pre-2023 challenges, where the Court of Appeal grappled with authenticating electronic banking records and SMS transaction alerts under the restrictive framework of the original Evidence Act. Similarly, in *MTN Nigeria Communications Ltd v. Aderotimi*[4], the Supreme Court faced difficulties in determining the admissibility of call data records and electronic communications logs.

President Bola Ahmed Tinubu assent to the Evidence (Amendment) Act 2023 on June 12, 2023,[5] marked a watershed moment in Nigerian jurisprudence. The Act introduced

---

[1] Foundation Chambers, *Revolutionizing Evidence Gathering, An Overview of the Evidence (Amendment) Act 2023*, by Emmanuel Ikwuakolam (25 August 2023). Available at: https://foundationchambers.com/revolutionizing-evidence-gathering-an-overview-of-the-evidence-amendment-act-2023-emmanuel-ikwuakolam/ accessed 12 September 2025.
[2] Stren & Blan Partners, *Evidence (Amendment) Act 2023, Aligning Evidence Taking in Judicial Proceedings with Technological Advancements*. Available at: https://strenandblan.com/evidence-amendment-act-2023-aligning-evidence-taking-in-judicial-proceedings-with-technological-advancements/ accessed 12 September 2025.
[3] (2018) LPELR-46234(CA).
[4] (2017) LPELR-43456(SC).
[5] *Supra note 1.*

comprehensive definitions for digital terms and established four new sections (84A-84D) that fundamentally altered the landscape of electronic evidence in Nigerian courts.[6]

1.2 Statement of the Problem

Despite the significant legislative reforms introduced by the Evidence (Amendment) Act 2023, several critical issues remain unresolved regarding the role of digital evidence in Nigerian legal proceedings: The transition from the restrictive provisions of Section 84 of the Evidence Act 2011 to the more liberal framework under sections 84A-84D has created interpretational challenges for practitioners and judges.[7] While the new Act recognizes electronic records as admissible evidence,[8] questions persist regarding the specific authentication requirements for different types of digital evidence.

The credibility of digital evidence presents unique challenges distinct from traditional documentary evidence[9]. Issues such as data integrity, metadata preservation, chain of custody for electronic records, and the potential for digital manipulation require specialized technical knowledge that many legal practitioners and judicial officers currently lack[10].

Nigeria's inconsistent technological infrastructure may impede uniform implementation of digital evidence provisions across different court jurisdictions[11]. Rural courts may lack the necessary equipment to properly examine electronic evidence, potentially creating disparities in access to justice. The increased reliance on digital evidence raises concerns about

---

[6] DOA Law Firm, *A Review of the Evidence Act (Amendment) Act, 2023* (30 August 2023). Available at: https://www.doa-law.com/evidence-act/ accessed 12 September 2025.
[7] *Supra* note 5.
[8] Evidence (Amendment) Act 2023, Section 84A.
[9] *Supra* note 2.
[10] *Supra* note 5
[11] *Ibid.*

cybersecurity vulnerabilities and the potential for sophisticated digital fraud[12]. The legal system must develop mechanisms to detect and prevent the presentation of manipulated or fabricated electronic evidence.

1.3 Research Questions

This study addresses the following research questions:

1. How do the provisions of sections 84A-84D of the Evidence (Amendment) Act 2023 transform the admissibility standards for digital evidence in Nigerian courts?
2. What are the current challenges in assessing the credibility of digital evidence within the Nigerian legal system?
3. How do Nigerian courts authenticate different types of electronic records, and what standards should be applied for various digital evidence formats?
4. What impact has the Evidence (Amendment) Act 2023 had on litigation practices and outcomes in Nigerian courts?
5. How does Nigeria's approach to digital evidence compare with international best practices and standards?
6. What recommendations can be made to enhance the effective implementation of digital evidence provisions in Nigerian legal proceedings?

1.4 Aim and Objectives

This study aims to examine the role of digital evidence in Nigerian legal proceedings, focusing on admissibility and credibility issues under the Evidence (Amendment) Act 2023.

[12] *Ibid*

The specific objectives are to:

1. Analyze the legal framework governing digital evidence admissibility
2. Evaluate the challenges and opportunities presented by the new provisions
3. Assess judicial interpretation and application of sections 84A-84D
4. Examine authentication requirements for electronic records and digital signatures
5. Investigate the impact of technical infrastructure limitations
6. Propose practical recommendations for enhancing credibility assessment of digital evidence in Nigerian courts.

By achieving these objectives, the study will provide a comprehensive understanding of the role of digital evidence in Nigerian legal proceedings and identify areas for improvement.

1.5 Scope and limitation of the study.

The review of current literature reveals several significant gaps that this research aims to address. Firstly, there is a notable lack of comprehensive analysis of the new sections (84A-84D) of the Evidence (Amendment) Act 2023. While various aspects of digital evidence have been discussed, no existing study provides a thorough examination of all four sections collectively. This gap highlights the need for an integrated analysis to understand the full implications of these provisions.

Furthermore, most existing commentary on the Evidence (Amendment) Act 2023 consists of doctrinal analysis, with limited empirical research examining the practical challenges of implementing the new digital evidence provisions. This research will contribute to filling this gap by providing empirical insights into the real-world application of these laws.

1.6 Significance of the Study

This study on the role of digital evidence in legal proceedings, focusing on admissibility and credibility in the Nigerian legal system, is significant because it contributes to the development of a more robust legal framework for digital evidence in Nigeria. By examining the effectiveness of the Evidence (Amendment) Act 2023, the study identifies areas for improvement, providing valuable insights for policymakers, lawmakers, and legal practitioners. This research will help to clarify the legal requirements for the admissibility of digital evidence, ensuring that the legal system is equipped to handle the complexities of digital evidence in a fair and efficient manner.

The study enhances judicial understanding of digital evidence complexities, enabling judges, lawyers, and law enforcement agencies to handle digital cases more effectively. By analyzing judicial interpretation and application of digital evidence provisions, the study provides practical guidance on how to navigate the challenges and opportunities presented by digital evidence. This will ultimately lead to more informed decision-making and improved outcomes in cases involving digital evidence.

Furthermore, the study informs strategies to improve access to justice, particularly in cases involving digital evidence, promoting fairness in legal proceedings. By examining the impact of digital evidence on access to justice, the study highlights the need for equal access to digital technologies and expertise, ensuring that all parties have a fair opportunity to present their case.

The study's findings and recommendations also advance digital forensics and cybersecurity in Nigeria, supporting the development of more secure and reliable digital systems. By exploring

the technical aspects of digital evidence, the study contributes to the advancement of digital forensics, enabling law enforcement agencies and legal practitioners to better understand and utilize digital evidence.

Moreover, this research has implications for the broader Nigerian society, as it will help to promote trust and confidence in the legal system. By ensuring that the legal system is equipped to handle digital evidence in a fair and efficient manner, the study contributes to the rule of law and the protection of individual rights.

Overall, this study is crucial for promoting justice, fairness, and efficiency in legal proceedings involving digital evidence in Nigeria. Its findings and recommendations will provide valuable insights for policymakers, lawmakers, legal practitioners, and law enforcement agencies, ultimately contributing to a more just and equitable society.

1.7 Research Methodology

This project employs a comprehensive legal research methodology to examine the role of digital evidence in Nigerian legal proceedings. The approach combines doctrinal analysis, case law research, empirical research, and stakeholder engagement to provide a thorough understanding of the subject. Doctrinal Analysis conducts a systematic examination of the Evidence (Amendment) Act 2023 provisions, analyzing legislative intent, drafting history, and integration with broader Nigerian evidence law principles and the case law research is a comprehensive review of Nigerian court decisions involving digital evidence is undertaken, analyzing judicial interpretation patterns and appellate court guidance on authentication standards. And others which includes the Empirical Research, Stakeholder Engagement

By combining these approaches, the study provides a comprehensive understanding of digital evidence in Nigerian courts, highlighting challenges, opportunities, and areas for improvement.

1.8 Chapter Synopsis

This work is divided into five chapters, each building upon the other to provide a coherent discussion of the subject. Chapter one introduces the research topic by outlining the background and significance of digital evidence in modern legal systems. It states the research problem, objectives, research questions, scope, and methodology. The chapter also highlights the justification for the study and briefly explains the structure of the work.

Chapter two reviews existing literature on digital evidence and its application in legal proceedings. It explores scholarly opinions, judicial perspectives, and existing gaps in research. It also sets out the theoretical frameworks guiding the study, such as legal positivism and the reliability theory of evidence.

Chapter three critically analyses the legal principles governing the admissibility of digital evidence in court. It discusses statutory provisions, case law, and procedural requirements, particularly focusing on conditions under the Evidence Act, 2011 and relevant judicial pronouncements.

Chapter four examines the factors that influence the credibility and reliability of digital evidence, including issues of authentication, chain of custody, and expert analysis. It also explores how courts evaluate digital evidence in criminal and civil matters.

Finally, Chapter five summarizes key findings, draws conclusions from the analysis, and provides practical recommendations for improving the handling of digital evidence in legal proceedings. It suggests reforms in law, policy, and practice to enhance both admissibility and credibility.

CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

The exponential growth of digital technology has fundamentally transformed the landscape of evidence collection, preservation, and presentation in legal proceedings. Digital evidence, defined as information stored or transmitted in binary form that may be relied upon in court, has become increasingly central to modern litigation across criminal, civil, and administrative contexts.[13] This chapter provides a comprehensive review of existing literature on digital evidence, examining its historical development, typology, legal frameworks, and the theoretical foundations that underpin its admissibility and credibility in court proceedings.

The admissibility of digital evidence presents unique challenges that distinguish it from traditional forms of evidence. Unlike physical evidence, digital data is inherently volatile, easily alterable, and often requires specialized technical knowledge to collect, preserve, and interpret.[14] These characteristics have necessitated the development of specific legal standards and procedural safeguards to ensure that digital evidence admitted in court is both reliable and authentic. The credibility of digital evidence, meanwhile, depends not only on its technical

---

[13] E, Casey. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press, p. 7. Available at: https://www.sciencedirect.com/book/9780123742681/digital-evidence-and-computer-crime Accessed: 8 November 2025.

[14] National Institute of Standards and Technology (2006). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86, p. 2-1. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf Accessed: 8 November 2025.

integrity but also on the chain of custody, the methods of collection and analysis, and the qualification of expert witnesses who interpret such evidence.[15]

This literature review synthesizes scholarly works, judicial pronouncements, and statutory provisions from multiple jurisdictions to provide a holistic understanding of how courts have grappled with the challenges posed by digital evidence. Particular attention is paid to the Nigerian legal framework, while drawing comparative insights from jurisdictions such as the United States, the United Kingdom, and other Commonwealth countries that have developed sophisticated jurisprudence in this area. The chapter also identifies critical gaps in the current literature that warrant further scholarly investigation.

2.2 Historical Development of Digital Evidence

The evolution of digital evidence in legal proceedings mirrors the broader trajectory of technological advancement over the past five decades. The earliest instances of digital evidence in courtrooms emerged in the 1970s, when mainframe computer records began to be introduced as business documents.[16] However, it was not until the widespread adoption of personal computers in the 1980s that courts were forced to confront fundamental questions about the nature, reliability, and admissibility of electronically stored information.

2.2.1 The Pioneering Era (1970s-1990s)

The seminal case of *King v. State*[17] in 1980 represented one of the first instances where an American appellate court addressed the admissibility of computer-generated evidence. The Indiana Court of Appeals held that computer printouts could be admitted under the business records exception to the hearsay rule, provided that proper foundation was established

[15] S, Mason. (ed.) (2017). *Electronic Evidence* (4th ed.). LexisNexis, pp. 15-18. Available at: https://www.lexisnexis.co.uk/products/electronic-evidence.html Accessed: 8 November 2025.
[16] Kerr OS, 'Digital Evidence and the New Criminal Procedure' (2005) 105(1) *Columbia Law Review* 279, 285. Available at: https://columbialawreview.org/content/digital-evidence-and-the-new-criminal-procedure/ Accessed: 8 November 2025.
[17] *King v. State*, 222 Ind. 168, 388 N.E.2d 118 (1980).

regarding the reliability of the computer system. This decision established a precedent that would influence subsequent judicial approaches to digital evidence for decades.

In the United Kingdom, the Police and Criminal Evidence Act 1984 (PACE) was among the first legislative attempts to address the admissibility of computer-generated evidence.[18] Section 69 of PACE originally required that for computer-generated evidence to be admissible, it had to be shown that the computer was operating properly and that there were no reasonable grounds to believe it was not functioning correctly. Although this provision was later repealed by the Youth Justice and Criminal Evidence Act 1999, it represented a significant early effort to establish specific standards for digital evidence.[19]

2.2.2 The Internet Age (1990s-2000s)

The proliferation of the internet in the 1990s exponentially increased the volume and variety of digital evidence. Email communications, website content, and digital transactions became routine subjects of litigation. The landmark case of *Lorraine v. Markel American Insurance Co.*[20] in 2007 provided comprehensive guidance on the authentication and admissibility of electronic evidence under the Federal Rules of Evidence, establishing that digital evidence must be evaluated under the same framework as traditional evidence, with appropriate consideration for its unique characteristics.

In Nigeria, the Evidence Act 2011 marked a watershed moment in the legal treatment of digital evidence. The Act, which repealed the colonial-era Evidence Act of 1945, introduced specific provisions for the admissibility of electronic evidence in sections 83-84 and 93-94.[21] Section 84 specifically addresses computer-generated evidence, providing that a statement

---

[18] Police and Criminal Evidence Act 1984 (UK), c. 60, s. 69.
[19] Youth Justice and Criminal Evidence Act 1999 (UK), c. 23, s. 60, Sch. 3.
[20] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007).
[21] Evidence Act 2011 (Nigeria), ss. 83-84, 93-94.

contained in a document produced by a computer is admissible as evidence of any fact stated therein if it can be shown that the computer was operating properly.[22]

2.2.3 The Mobile and Cloud Computing Era (2010s-Present)

The advent of smartphones, cloud computing, and social media platforms has created new frontiers for digital evidence. In *Riley v. California*,[23] the United States Supreme Court recognized that modern cell phones are not just communication devices but repositories of vast amounts of personal information, holding that warrantless searches of cell phones incident to arrest are unconstitutional. This decision acknowledged the unique privacy interests implicated by digital devices and has influenced digital evidence jurisprudence globally.

The Nigerian case of *Dickson v. Sylva*[24] demonstrated the evolving judicial attitude toward digital evidence in Nigerian courts. The Court of Appeal admitted electronic evidence in the form of text messages and call logs, emphasizing that such evidence must meet the requirements of authenticity, relevance, and proper certification as outlined in the Evidence Act 2011. This case represents the growing acceptance of diverse forms of digital evidence in Nigerian jurisprudence.

2.3 Types of Digital Evidence

Digital evidence encompasses a broad spectrum of electronically stored information that can be presented in legal proceedings. Understanding the typology of digital evidence is essential for appreciating the distinct challenges each category presents regarding admissibility and credibility.

2.3.1 Computer-Generated Evidence

---

[22] Evidence Act 2011 (Nigeria), s. 84(1).
[23] *Riley v. California*, 573 U.S. 373 (2014).
[24] *Dickson v. Sylva* (2015) LPELR-24503(CA).

Computer-generated evidence refers to data produced by computer systems without direct human input, such as automated logs, timestamps, and system-generated reports.[25] This category includes server logs, GPS location data, automated financial transactions, and sensor data from Internet of Things (IoT) devices. The reliability of such evidence depends heavily on the proper functioning of the computer system that generated it.

In *R v. Cochrane*,[26] the English Court of Appeal addressed the admissibility of computer-generated evidence in the context of electronic till receipts. The court held that such evidence could be admitted under the business records exception, provided that the party tendering the evidence could demonstrate the reliability of the computer system. This approach has been influential in Commonwealth jurisdictions, including Nigeria.

2.3.2 Computer-Stored Evidence

Computer-stored evidence comprises information created by human users and stored in digital format, including word processing documents, spreadsheets, emails, and digital photographs.[27] This type of evidence is analogous to traditional documentary evidence but exists in electronic form. The case of *United States v. Safavian*[28] established important precedents for authenticating emails and other computer-stored documents, emphasizing the need to verify authorship and the integrity of the document from creation to presentation in court.

2.3.3 Digital Communications

---

[25] Chaikin D and Koenig E, 'Admissibility of Electronic Business Records' (2010) 33(1) *University of New South Wales Law Journal* 30, 35. Available at: http://www.unswlawjournal.unsw.edu.au/ Accessed: 8 November 2025.

[26] *R v. Cochrane* [1993] Crim LR 48 (CA). Available at: https://www.lexisnexis.co.uk/legal/ Accessed: 8 November 2025.

[27] Sommer P, 'Directors' Responsibilities and Authentication of Digital Evidence' (2008) 5(1-2) *Digital Investigation* 43. Available at: https://www.sciencedirect.com/science/article/pii/S174228760800013X Accessed: 8 November 2025.

[28] *United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006). Available at: https://casetext.com/case/us-v-safavian-9 Accessed: 8 November 2025.

Digital communications represent a rapidly growing category of evidence that includes emails, text messages, instant messages, social media posts, and Voice over Internet Protocol (VoIP) communications.[29] The case of *Davids v. City of Las Vegas*[30] addressed the admissibility of text messages, holding that such evidence must be authenticated through circumstantial evidence demonstrating that the messages were sent and received by the purported parties.

In Nigeria, the case of *APC v. INEC*[31] involved the presentation of WhatsApp messages and social media posts as evidence of electoral malpractice. While the tribunal admitted this evidence, it emphasized the need for proper authentication and certification in accordance with section 84 of the Evidence Act 2011, demonstrating the growing importance of digital communications in Nigerian litigation.

2.3.4 Metadata

Metadata, often described as "data about data," includes information such as creation dates, modification dates, author information, and location data embedded within digital files.[32] The evidentiary value of metadata was recognized in *Williams v. Sprint/United Management Co.*,[33] where the court admitted metadata from electronic documents to establish timelines and authorship. However, the court cautioned that metadata can be easily manipulated, necessitating careful authentication procedures.

2.3.5 Digital Images and Video

---

[29] Shearing V and Macaulay R, 'Text Messages as Evidence' (2020) 15(2) *Journal of Digital Forensics, Security and Law* 95. Available at: https://commons.erau.edu/jdfsl/ Accessed: 8 November 2025.
[30] *Davids v. City of Las Vegas*, 2013 WL 1622555 (D. Nev. Apr. 15, 2013)
[31] *APC v. INEC* (2020) LPELR-49567(CA).
[32] Garrie DB and Gelb M, *E-Discovery & Digital Evidence: Cases and Materials* (Thomson West 2007) 234. Available at: https://legal.thomsonreuters.com/ Accessed: 8 November 2025.
[33] *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640 (D. Kan. 2005). Available at: https://casetext.com/case/williams-v-sprint-united-management-co Accessed: 8 November 2025.

Digital photographs and video recordings present unique challenges due to the ease with which they can be manipulated using editing software.[34] The case of *State v. Swinton*[35] established a framework for authenticating digital photographs, requiring testimony that the image fairly and accurately represents what it purports to depict and has not been altered. The increasing sophistication of deepfake technology has further complicated the credibility assessment of digital images and videos.

2.3.6 Cryptocurrency and Blockchain Evidence

The emergence of cryptocurrencies and blockchain technology has created novel forms of digital evidence.[36] Blockchain records, by their nature, are designed to be immutable and transparent, potentially offering enhanced reliability compared to traditional digital evidence. However, courts are still developing frameworks for evaluating such evidence. The case of *Tulip Trading Ltd v. Bitcoin Association*[37] in the UK addressed the evidentiary treatment of blockchain records, recognizing their potential reliability while acknowledging the technical complexity involved in presenting such evidence.

2.4 Legal Frameworks Governing Digital Evidence

The admissibility and treatment of digital evidence is governed by statutory provisions, rules of procedure, and judicial precedents that vary across jurisdictions. This section examines the key legal frameworks applicable to digital evidence, with particular focus on the Nigerian context and comparative insights from other jurisdictions.

2.4.1 The Nigerian Evidence Act 2011

---

[34] Farid H, 'Image Forgery Detection' (2009) 26(2) *IEEE Signal Processing Magazine* 16. Available at: https://ieeexplore.ieee.org/document/4786596 Accessed: 8 November 2025.
[35] *State v. Swinton*, 847 A.2d 921 (Conn. 2004).
[36] Houben R and Snyers A, 'Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion' (2020) *European Parliament Study* 67-72. Available at : https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf Accessed: 8 November 2025.
[37] *Tulip Trading Ltd v. Bitcoin Association* [2022] EWHC 141 (Ch).

The Evidence Act 2011 represents the primary statutory framework governing the admissibility of evidence in Nigerian courts. The Act introduced comprehensive provisions specifically addressing electronic evidence, marking a significant departure from the colonial Evidence Act of 1945.[38]

Section 84: Admissibility of Computer-Generated Evidence

Section 84(1) of the Evidence Act provides: "In any proceedings, a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated therein 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."[39] Subsection (2) outlines the foundational requirements, including that the computer was operating properly and that the information was supplied to the computer in the ordinary course of activities.

The case of *Registered Trustees of National Association of Community Health Practitioners of Nigeria v. Medical and Health Workers Union of Nigeria*[40] provided judicial interpretation of section 84, holding that computer-generated evidence must be accompanied by a certificate identifying the document, describing the manner in which it was produced, and providing particulars of the device involved in its production.

Section 83: Proof of Documents by Production of Copies

Section 83 addresses the production of copies of documents, including electronic copies. It provides that a document may be proved by the production of a copy authenticated by a

[38] Aguda TA, *The Law of Evidence in Nigeria* (Spectrum Books 1999) 245.
[39] Evidence Act 2011 (Nigeria), s. 84(1).
[40] *Registered Trustees of National Association of Community Health Practitioners of Nigeria v. Medical and Health Workers Union of Nigeria* (2008) 2 NWLR (Pt. 1072) 575.

certificate or otherwise, expanding the traditional "best evidence rule" to accommodate electronic documents.[41]

Section 93: Admissibility of Electronic Communications

Section 93 specifically addresses the admissibility of evidence generated by means of electronic communication, making such evidence admissible notwithstanding any rule requiring proof that such evidence did not originate from the stated source.[42] However, this provision is subject to meeting authentication requirements.

2.4.2 The Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

The Cybercrimes Act provides additional procedural mechanisms relevant to digital evidence, particularly in criminal proceedings involving cyber offenses.[43] Section 44 grants law enforcement agencies powers to obtain real-time collection of traffic data, while section 45 addresses the preservation of computer data. Section 46 provides for production orders compelling service providers to submit specified computer data in their possession.

The case of *Sambo Dasuki v. FRN*[44] involved the application of the Cybercrimes Act in relation to electronic evidence obtained from mobile devices and computers. The court emphasized that evidence obtained through the procedures outlined in the Act, including proper preservation and chain of custody, would be admissible, while evidence obtained through unauthorized means could be excluded.

2.4.3 International and Comparative Frameworks

United States: Federal Rules of Evidence

---

[41] Evidence Act 2011 (Nigeria), s. 83(1)-(3).
[42] Evidence Act 2011 (Nigeria), s. 93(1).
[43] Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria). Available at: https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf Accessed: 8 November 2025.
[44] *Sambo Dasuki v. FRN* (2016) LPELR-41116(CA).

The United States Federal Rules of Evidence, particularly Rules 401-403 (relevance), Rule 801 (hearsay), and Rule 901 (authentication), provide the foundational framework for digital evidence admissibility in federal courts.[45] The 2006 amendments to the Federal Rules of Civil Procedure specifically addressed electronically stored information (ESI), introducing provisions for discovery, preservation, and production of digital evidence.[46]

The landmark decision in *Daubert v. Merrell Dow Pharmaceuticals*[47] established the standard for expert testimony, which is frequently necessary for presenting and interpreting complex digital evidence. The Daubert standard requires that expert testimony be based on scientifically valid reasoning and methodology, a requirement that applies to digital forensic experts.

[45] Federal Rules of Evidence (US), Rules 401-403, 801, 901. Available at: https://www.law.cornell.edu/rules/fre Accessed: 8 November 2025.
[46] Federal Rules of Civil Procedure (US), Rule 34(a)(1)(A) (2006 amendments). Available at: https://www.law.cornell.edu/rules/frcp Accessed: 8 November 2025.
[47] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993). Available at: https://supreme.justia.com/cases/federal/us/509/579/ Accessed: 8 November 2025.

United Kingdom: Civil Evidence Act 1995 and Criminal Justice Act 2003

In the United Kingdom, the Civil Evidence Act 1995 abolished the common law hearsay rule in civil proceedings, significantly simplifying the admission of digital evidence in civil cases.[48] The Criminal Justice Act 2003 modernized the hearsay provisions in criminal cases, with specific provisions addressing computer records under section 129.[49]

The case of *R v. Maqsud Ali*[50] established the principle that mechanical instruments such as computers are presumed to be in order unless there is evidence to the contrary, creating a rebuttable presumption of reliability for computer-generated evidence.

European Union: General Data Protection Regulation (GDPR)

While not directly governing admissibility, the GDPR has significant implications for the collection and presentation of digital evidence in European jurisdictions.[51] The regulation imposes strict requirements on data processing, storage, and transfer, which can affect the legality of evidence gathering and potentially its admissibility in court.

Convention on Cybercrime (Budapest Convention)

The Council of Europe's Convention on Cybercrime, to which several African nations are parties, provides international cooperation mechanisms for digital evidence.[52] Articles 14-21 establish procedural powers for the preservation, search, seizure, and disclosure of computer data, facilitating cross-border investigations involving digital evidence.

2.4.4 Admissibility Requirements for Digital Evidence

---

[48] Civil Evidence Act 1995 (UK), c. 38. Available at: https://www.legislation.gov.uk/ukpga/1995/38/contents accessed: 8 November 2025.
[49] Criminal Justice Act 2003 (UK), c. 44, s. 129. Available at: https://www.legislation.gov.uk/ukpga/2003/44/section/129 Accessed: 8 November 2025.
[50] *R v. Maqsud Ali* [1966] 1 QB 688.
[51] Regulation (EU) 2016/679 (General Data Protection Regulation), Arts. 5-6. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 Accessed: 8 November 2025.
[52] Council of Europe Convention on Cybercrime (Budapest Convention), 23 November 2001, ETS No. 185, Arts. 14-21. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention Accessed: 8 November 2025.

Across jurisdictions, digital evidence must generally satisfy several foundational requirements to be admissible:

Relevance

Digital evidence must be relevant to the issues in dispute. In *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*,[53] the court emphasized that even authentic digital evidence may be excluded if it is not relevant to the claims or defenses in the case.

Authentication

Authentication is perhaps the most critical requirement for digital evidence. The proponent must establish that the evidence is what it purports to be.[54] In the Nigerian case of *Buhari v. INEC*,[55] the Supreme Court held that electronic evidence must be properly authenticated through direct evidence, circumstantial evidence, or expert testimony before it can be admitted.

Integrity and Chain of Custody

The integrity of digital evidence from collection to presentation must be demonstrated through proper chain of custody documentation.[56] The case of *State v. Cook*[57] held that the proponent of digital evidence must show that the evidence has not been altered or tampered with, typically through testimony regarding forensic imaging procedures and hash value verification.

Hearsay Considerations

---

[53] *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004). Available at: https://www.courtlistener.com/ Accessed: 8 November 2025.
[54] Imwinkelried EJ, 'Authenticating Digital Evidence' (2005) 20(2) *Criminal Justice* 2. Available at: https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/ Accessed: 8 November 2025.
[55] *Buhari v. INEC* (2008) 19 NWLR (Pt. 1120) 246 at 340-342. Available at: https://www.lawpavilion.com (Accessed: 8 November 2025).
[56] Mohay G et al, *Computer and Intrusion Forensics* (Artech House 2003) 89. Available at: https://us.artechhouse.com/ Accessed: 8 November 2025.
[57] *State v. Cook*, 145 Wash. App. 784, 187 P.3d 1151 (2008).

Digital evidence often implicates hearsay rules, as the information was typically generated or recorded outside of court.[58] However, various exceptions to the hearsay rule, such as the business records exception, may apply. The case of *United States v. Hassan*[59] addressed the application of hearsay exceptions to social media posts, holding that posts made by party-opponents are admissible as statements against interest.

Best Evidence Rule

The best evidence rule traditionally required the production of original documents. Modern evidence codes have adapted this rule for electronic evidence, generally allowing certified copies or printouts of electronic data.[60] Section 83 of the Nigerian Evidence Act addresses this issue, providing flexibility for the proof of electronic documents through authenticated copies.

2.5 Theoretical Framework

The analysis of digital evidence admissibility and credibility benefits from grounding in established theoretical frameworks that provide coherent explanatory models for understanding evidentiary principles and their application to novel forms of evidence.

2.5.1 The Rationalist Theory of Evidence

The rationalist theory of evidence, articulated by scholars such as Twining and Wigmore, posits that the primary function of evidence law is to facilitate accurate fact-finding through rational inference.[61] Under this framework, evidence is admissible if it has logical probative value that outweighs potential prejudicial effects. This theory provides a useful lens for

---

[58] Park RC, 'The Hearsay Rule and the Stability of Verdicts: A Response to Professor Nesson' (2007) 70(4) *Minnesota Law Review* 1057. Available at: https://scholarship.law.umn.edu/mlr/ Accessed: 8 November 2025.
[59] *United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014).
[60] Lempert RO, Gross SR and Liebman JS, *A Modern Approach to Evidence* (3rd edn, West Publishing 2000) 1226. Available at: https://legal.thomsonreuters.com/ Accessed: 8 November 2025.
[61] Twining W, *Rethinking Evidence: Exploratory Essays* (Northwestern University Press 1990) 71. Available at: https://nupress.northwestern.edu/ Accessed: 8 November 2025.

analyzing digital evidence, as it focuses on the logical connection between the evidence and the proposition to be proved.

Applied to digital evidence, the rationalist approach suggests that technical evidence demonstrating the reliability of computer systems, the authenticity of digital files through hash value comparison, and the integrity of chain of custody procedures all serve to establish the rational basis for drawing inferences from digital evidence. The theory supports a flexible, case-by-case approach to admissibility that considers the specific characteristics of each piece of digital evidence rather than applying rigid categorical rules.

2.5.2 The Procedural Justice Theory

Procedural justice theory, developed by psychologists and legal scholars including Tyler and Lind, emphasizes the importance of fair procedures in legal decision-making.[62] This theory is particularly relevant to digital evidence because the technical complexity of such evidence can create information asymmetries between parties, potentially undermining procedural fairness. The theory suggests that admissibility rules for digital evidence should incorporate procedural safeguards such as mandatory disclosure of digital forensic methodologies, opportunities for opposing parties to examine and challenge digital evidence, and appointment of neutral experts in cases involving highly technical evidence. The Nigerian Evidence Act's requirement for certification under section 84(4) can be understood as a procedural justice mechanism that ensures opposing parties are adequately informed about the nature and provenance of computer-generated evidence.[63]

2.5.3 The Reliability Theory

---

[62] Tyler TR, 'Procedural Justice, Legitimacy, and the Effective Rule of Law' (2003) 30 *Crime and Justice* 283. available at: https://www.journals.uchicago.edu/toc/cj/current Accessed: 8 November 2025.
[63] Evidence Act 2011 (Nigeria), s. 84(4).

The reliability theory, reflected in cases such as *Daubert v. Merrell Dow Pharmaceuticals*,[64] holds that expert testimony and scientific evidence should be admitted only if the underlying methodology is scientifically valid and can be reliably applied to the facts at issue. This theory is particularly apt for digital forensic evidence, which relies heavily on technical methodologies for data extraction, analysis, and interpretation.

Under the reliability framework, courts should evaluate digital evidence based on factors such as: (1) whether the forensic methodology has been tested and peer-reviewed; (2) the known or potential error rate of the technique; (3) the existence of standards governing the methodology; and (4) the degree of acceptance within the relevant scientific community.[65] The International Organization on Computer Evidence (IOCE) and the Scientific Working Group on Digital Evidence (SWGDE) have developed standards for digital forensic practice that provide benchmarks for evaluating reliability.[66]

2.5.4 The Authenticity Theory

The authenticity theory, grounded in traditional evidence doctrine, requires that evidence be genuine, that it is what its proponent claims it to be.[67] For digital evidence, authenticity is complicated by the ease of creating, copying, and altering digital files. The theory requires a showing of authenticity before evidence can be admitted, but does not prescribe the means of authentication.

---

[64] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
[65] Risinger DM, 'Navigating Expert Reliability: Are Criminal Standards of Certainty Being Left on the Dock?' (2000) 64(1) *Albany Law Review* 99. Available at: https://www.albanylawreview.org/ Accessed: 8 November 2025.
[66] Scientific Working Group on Digital Evidence, *SWGDE Best Practices for Computer Forensics* (2016). Available at: https://drive.google.com/file/d/1M_OWBlF5fikNH2BREaoBoHKlRF0L0N5i/view Accessed: 8 November 2025.
[67] Wigmore JH, *A Treatise on the Anglo-American System of Evidence in Trials at Common Law* (3rd edn, Vol 7, Little, Brown and Company 1940). Available at: https://archive.org/ Accessed: 8 November 2025.

Scholars such as Mason have argued that digital evidence requires enhanced authentication procedures due to its unique characteristics.[68] This has led to the development of technical authentication methods specific to digital evidence, including cryptographic hash functions that create unique digital "fingerprints" of files, digital signatures that verify the identity of document creators, and forensic imaging techniques that create exact copies of digital storage media.

The authentication requirement reflects an underlying concern with evidence tampering and fabrication. In the digital context, this concern is heightened by the possibility of sophisticated manipulations that leave no visible trace. The case of *Lorraine v. Markel American Insurance Co.*[69] emphasized that authentication of electronic evidence requires consideration of factors such as the chain of custody, the security of the storage system, and any evidence of tampering or alteration.

2.5.5 The Four Corners Rule and Digital Evidence

The "four corners rule" traditionally holds that a document's meaning should be determined solely from its content without resort to extrinsic evidence.[70] However, this rule has been challenged in the context of digital evidence, where metadata, system logs, and other extrinsic digital artifacts may be essential to understanding and authenticating a document.

---

[68] Mason S and Seng D (eds), *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies 2017) 67-89. Available at: https://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence Accessed: 8 November 2025.

[69] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 546 (D. Md. 2007).

[70] Corbin AL, 'The Interpretation of Words and the Parol Evidence Rule' (1944) 50(2) *Cornell Law Quarterly* 161. Available at: https://scholarship.law.cornell.edu/clr/ Accessed: 8 November 2025.

Scholars such as Kerr have argued for a reformulation of traditional evidence doctrines to account for the unique nature of digital evidence.[71] This theoretical work has influenced judicial approaches, with courts increasingly recognizing that understanding digital evidence requires consideration of technical context beyond the "four corners" of a digital document.

2.5.6 The Integration Theory

The integration theory, proposed by Park and others, suggests that evidence law should integrate technological developments rather than resist them, adapting traditional doctrines to accommodate new forms of evidence while maintaining core evidentiary principles.[72] This approach is reflected in statutes such as the Nigerian Evidence Act 2011, which incorporated provisions specifically addressing electronic evidence while retaining fundamental concepts such as relevance, authentication, and hearsay.

The integration approach recognizes that digital evidence is not categorically different from traditional evidence in its essential nature, both serve as means of proving or disproving facts in litigation. However, the approach acknowledges that the unique characteristics of digital evidence may require modified procedures and standards. For example, while the best evidence rule traditionally required production of original documents, the integration approach recognizes that the concept of an "original" is meaningless for digital files that exist as strings of binary code, leading to acceptance of authenticated copies.[73]

---

[71] Kerr OS, 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution' (2004) 102(5) *Michigan Law Review* 801. Available at: https://repository.law.umich.edu/mlr/ Accessed: 8 November 2025.

[72] Park RC, Leonard DP and Goldberg SH, *Evidence Law, A Student's Guide to the Law of Evidence as Applied in American Trials* (2nd edn, West Publishing 2004) 634. Available at: https://legal.thomsonreuters.com/ Accessed: 8 November 2025.

[73] Goodman MD, 'Making Computer Stored Records Admissible' (2003) 12(1) *Information Systems Security* 8. Available at: https://www.tandfonline.com/toc/uiss20/current Accessed: 8 November 2025.

2.6 Gaps in Current Literature

Despite the growing body of literature on digital evidence, several significant gaps remain that warrant further scholarly investigation and empirical research.

2.6.1 Limited Empirical Research on Judicial Decision-Making

There is a paucity of empirical research examining how judges actually evaluate digital evidence in practice.[74] While numerous case law analyses document judicial decisions, few studies systematically investigate the factors that influence judges' admissibility determinations or credibility assessments of digital evidence. Empirical research could illuminate whether judges' technical literacy affects their treatment of digital evidence and whether there are systematic biases in how different types of digital evidence are evaluated.

In the Nigerian context, there is virtually no published empirical research on how trial courts apply the provisions of the Evidence Act 2011 to digital evidence. Such research would be valuable in identifying practical challenges in implementing the statutory framework and could inform future legislative reforms.

2.6.2 Insufficient Analysis of Emerging Technologies

The literature has not adequately addressed the evidentiary implications of emerging technologies such as artificial intelligence, blockchain, and Internet of Things (IoT) devices.[75] While some scholarship examines cryptocurrency evidence, comprehensive frameworks for

---

[74] Mnookin JL, 'Scripting Expertise, The History of Handwriting Identification Evidence and the Judicial Construction of Reliability' (2001) 87(8) *Virginia Law Review* 1723, 1728. Available at: https://www.virginialawreview.org/ Accessed: 8 November 2025.

[75] Casey, E. and Turnbull, B. (2018). 'Digital Evidence on Mobile Devices', in Casey, E. (ed.) *Handbook of Digital Forensics and Investigation*. Academic Press, pp. 165-196. Available at: https://www.elsevier.com/ Accessed: 8 November 2025.

evaluating AI-generated evidence, smart contract records, and data from interconnected IoT devices remain underdeveloped.

For example, how should courts evaluate evidence generated by machine learning algorithms? Can the "black box" nature of some AI systems be reconciled with traditional requirements for transparency in evidence production? The literature has not sufficiently grappled with these questions, leaving courts without clear guidance when confronting such evidence.

2.6.3 Cross-Border Digital Evidence Challenges

Although some literature addresses international cooperation in obtaining digital evidence, there is insufficient analysis of the admissibility implications when evidence is obtained from foreign jurisdictions with different legal standards.[76] Cloud computing has made it common for relevant evidence to be stored across multiple jurisdictions, raising complex questions about sovereignty, privacy laws, and procedural requirements.

The Nigerian literature particularly lacks analysis of how courts should handle digital evidence obtained from foreign cloud service providers or through mutual legal assistance treaties. Given Nigeria's growing digital economy, this represents a significant gap requiring scholarly attention.

2.6.4 The Credibility Gap: Jury and Judge Comprehension

[76] Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. International Telecommunication Union, pp. 245-267. Available at: https://www.itu.int/en/Pages/default.aspx Accessed: 8 November 2025.

There is limited research on how judges and juries comprehend technical digital evidence and whether their understanding affects credibility determinations.[77] Cognitive psychology research suggests that people have systematic biases in evaluating probabilistic evidence and technical testimony, but this research has not been extensively applied to digital evidence specifically.

In jurisdictions like Nigeria where judges sit without juries, there is almost no research examining whether judicial technical literacy programs improve outcomes in cases involving digital evidence. This represents an important area for empirical investigation.

2.6.5 Digital Evidence and Fundamental Rights

The literature inadequately addresses the tension between effective use of digital evidence and fundamental rights such as privacy, freedom of expression, and protection against self-incrimination.[78] While some scholarship examines privacy concerns, there is insufficient theoretical work integrating digital evidence law with constitutional rights frameworks.

In Nigeria, despite constitutional protections for privacy under section 37 of the 1999 Constitution (as amended),[79] there is limited scholarly analysis of how these protections should affect the admissibility of digital evidence obtained through surveillance, device searches, or data breaches. The intersection of digital evidence law and constitutional rights deserves more sustained academic attention.

2.6.6 Standardization and Best Practices

---

[77] Hans, V.P. and Reyna, V.F. (2011). 'To Dollars from Sense: Qualitative to Quantitative Translation in Jury Damage Awards', *Journal of Empirical Legal Studies*, 8(S1), pp. 120-147. Available at: https://onlinelibrary.wiley.com/journal/17401461 Accessed: 8 November 2025.

[78] Solove, D.J. (2007). '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy', *San Diego Law Review*, 44(4), pp. 745-772. Available at: https://digital.sandiego.edu/sdlr/ Accessed: 8 November 2025.

[79] Constitution of the Federal Republic of Nigeria 1999 (as amended), s. 37. Available at: https://www.wipo.int/edocs/lexdocs/laws/en/ng/ng014en.pdf Accessed: 8 November 2025.

While international organizations have developed standards for digital forensic practice, the literature lacks comprehensive analysis of how these standards should be incorporated into legal admissibility frameworks.[80] There is insufficient scholarly engagement with questions such as whether compliance with technical standards should be a prerequisite for admissibility or merely a factor in credibility assessment.

Moreover, there is minimal research on the effectiveness of different chain of custody protocols for digital evidence. Given the ease with which digital evidence can be altered, this represents a critical gap in ensuring evidence integrity.

2.6.7 Social Media Evidence

Although social media has become ubiquitous, the literature has not developed comprehensive frameworks for authenticating and evaluating social media evidence.[81] Questions remain about how to authenticate the source of social media posts, how to preserve ephemeral content such as stories and snaps, and how to contextualize social media communications that rely heavily on implied meanings and cultural references.

The Nigerian literature particularly lacks analysis of how to handle evidence from social media platforms popular in Africa, such as WhatsApp, which has become a primary means of communication but raises unique challenges for authentication and preservation.

2.6.8 Cost and Access to Justice

---

[80] ISO/IEC 27037:2012, *Information technology, Security techniques, Guidelines for identification, collection, acquisition and preservation of digital evidence*. Available at: https://www.iso.org/standard/44381.html Accessed: 8 November 2025.

[81] Orebaugh, A. and Allnutt, J. (2010). 'Classification of Instant Messaging Communications for Forensics Analysis', *International Journal of Forensic Computer Science*, 1(1), pp. 22-28. Available at: https://www.ijofcs.org/ Accessed: 8 November 2025.

There is insufficient attention to how the technical complexity and expense of properly collecting, preserving, and presenting digital evidence affects access to justice.[82] Digital forensic services can be prohibitively expensive, potentially creating advantages for well-resourced parties. The literature has not adequately examined how evidence law can be structured to mitigate these disparities or whether courts should appoint neutral experts in cases where one party lacks resources for digital forensic services.

2.6.9 Deepfakes and Manipulated Evidence

The emergence of sophisticated techniques for creating fake digital content, particularly through AI-generated deepfakes, has received insufficient scholarly attention.[83] While some literature acknowledges the problem, comprehensive frameworks for detecting and excluding manipulated digital evidence remain underdeveloped. This gap is particularly concerning given the rapidly advancing capabilities of generative AI technologies.

---

[82] Rhode, D.L. (2004). *Access to Justice*. Oxford University Press, pp. 87-112. Available at: https://global.oup.com/ Accessed: 8 November 2025.

[83] Chesney, R. and Citron, D.K. (2019). 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *California Law Review*, 107(6), pp. 1753-1820. Available at: https://www.californialawreview.org/ Accessed: 8 November 2025.

CHAPTER THREE

LEGAL AND INSTITUTIONAL FRAMEWORKS

3.1 Introduction

The legal and institutional framework of digital evidence centers on ensuring that digital information meets the fundamental evidentiary standards of relevance, authenticity and reliability. The admissibility of digital evidence is regulated by various laws and rules both internationally and nationally.

International country like Canada was the first to pass specific legal guidelines addressing computer crimes, which laid the foundation for digital evidence standards, with legislation introduced in 1983[84]. Other international countries also regulated their own laws addressing the admissibility and standards for electronic evidence.

The development of legal standards for digital evidence has been an ongoing, international process, including working groups and international bodies like the, International Organization for Standardization(ISO) , International Electro-technical Commission (IEC) and the Council of Europe, especially through the Budapest Convention on Cybercrime. International laws and institutions has established legal standards influencing the admissibility of digital evidence. These standards prove to be a necessity to ensure conformance and mutual compliance across geographical and jurisdictional borders.[85]

---

[84] International Standard, ISO/IEC 27037,first edition 15-10-2012. Available at https://amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf, accessed on December 9.

[85] Marthie, G and others, 'The Need for Digital Evidence Standardization', *International Journal of Digital Crime and Forensics*, 4(2), April-June 2012, accessed December 9

In Nigeria, the legal system structure on digital evidence is primarily influenced by international countries like England and India, with the Nigeria legal system historically deriving significant influence from the English law.

The Evidence Act is a major document regulating the admissibility of digital evidence in Nigeria, and it's greatly influenced by the Indian Evidence Act(1872) and the Civil Evidence Act of 1968. There are also various laws and institutions that are made to regulate and interpret digital evidence, these laws includes, National Information Technology Development Agency (NITDA) Act, Cyber Crimes (Prohibition, Prevention, etc) Act, National Digital Economy and E - Governance Act. Institutions like, Judiciary (for interpretation and application of the Evidence Act), National Information Technology Development Agency, Corporate Affairs Commission (CAC). These legal structures work in hand in hand to regulate digital evidence in Nigeria.[86]

3.2 International Legal Structures Regulating Digital Evidence

International legal structures established standardize rules and regulations aiding the conformance and mutual compliance across countries. There are standardize conventions and laws that governs the collection, seizure and analyst process of digital evidence, which further determine the admissibility, reliability and authenticity of digital evidence in a court proceeding.

These standards are also adopted by National laws of various geographical jurisdiction , aiding the development of their own laws on electronic evidence, setting standardized requirements to be met before electronic evidence are admissible.

[86] Introduction to Digital Forensics, by United Nation office on drugs and crime. Available at https://www.unodc.org accessed September 10th, 2025.

3.2.1 Key International Laws regulating Digital Evidence

1. Council of Europe Convention on Cybercrime (Budapest Convention) : This is the most significant and widely adopted international treaty addressing cybercrime and electronic evidence. It establishes common ground for, procedural powers, which requires signatory states to align their National laws to allow for the preservation of computer data, search and seizure of digital media, and the interpretation of data.

Also, cross-border cooperation by providing mechanisms for Mutual Legal Assistance (MLA) and establishing a daily contact network to ensure expedited cooperation in urgent cases involving volatile digital evidence.[87]

2. EU E-evidence Regulation and Directive: The European Union has adopted legislation to create a new system for the swift collection of electronic evidence in criminal matters across member states, addressing the challenges used by data stored in different jurisdictions.

3. U.S. CLOUD Act (Clarifying Lawful Overseas Use of Data Act): The U.S. federal law allows American law enforcement to compel U.S. based technology company to provide requested electronic data stored on servers outside of the country, while also creating a framework for qualifying foreign governments to make direct requests.[88]

3.2.2 Key Institutional Standards and Guidelines

4. ISO/IEC standards: The International Organization for Standardization and the International Electro-technical Commission (IEC) have published key technical standards

[87] ibid
[88] Human Right Center, UC Berkeley School of law,Berkeley Protocol on Digital Open Source Investigations. Available at https://www.ohchr.org

for digital forensics.

ISO/IEC 27037:2012 - provides guidelines for the identification, collection, acquisition and preservation of potential digital evidence, aiming to preserve its integrity and authenticity.

ISO/IEC 27042:2015 - offers guidelines for the analysis and interpretation phases of the digital evidence process.

5. The Berkeley Protocol on Digital Open Source Investigations describes the professional standards that should be applied in the identification, collection, preservation, analysis and presentation of digital open source information and its use in international criminal investigation and human right investigation.

International legal structures created the basis of the admissibility and credibility of digital evidence which has been recognized worldwide, and aiding the development of national laws on electronic evidence, establishing mutual rules for the admissibility of digital evidence.

3.3 Legal Recognition of Digital Evidence in UNCITRAL Model Law (MLEC)

The UNCITRAL Model Law of Electronic Commerce (MLEC) is a 1996 legal framework designed to remove hurdles and provide legal certainty for e-commerce by ensuring that electronic and paper-based transactions are treated equally, that is giving equal credibility and admissibility to electronic transactions as paper-based transactions. It achieves this through core principles of non- discrimination against electronic evidence documents, technological neutrality and functional equivalence. The law aims to harmonize domestic

legislation worldwide to facilitate cross-national trade by giving legal validity to electronic contracts, signatures and record keeping[89].

3.3.1 The Opinion of UNCITRAL Model Law on Digital Evidence

The UNCITRAL Model Law on Electronic Evidence provides a legal framework to ensure that electronic records are treated fairly and admissible in legal proceedings, establishing principles like the best evidence rule for electronic records. It applies the fundamental principles of non-discrimination, technological neutrality and functional equivalence, ensuring that a record is not denied legal effect solely because it is in electronic form. The law is designed to harmonize national laws and international trade by addressing the legal admissibility and credibility of electronic evidence. Nigeria has not fully enacted a single comprehensive law directly embodied after the UNCITRAL Model Law on electronic evidence as a separate piece of legislation. Instead, its principles has influenced and has been incorporated into existing domestic laws, primarily the Evidence Act 2011, to govern the admissibility and treatment of Electronic records in legal proceedings. The UNCITRAL Model Law has awarded the use of electronic evidence in a court proceeding a solid credibility and admissibility equal to paper-based evidence. The UNCITRAL Model Law provides a legal recognition to electronic evidence globally.

In summary, Nigeria addresses electronic evidence through its general Evidence Act, leveraging in the core principles of UNCITRAL Model Law to provide a more modernize legal framework.[90]

---

[89] UNCITRAL Model Law on Electronic Commerce, Available at UNCITRAL,un.org, accessed December 10
[90] Guidelines on the treatment of Electronic Evidence in Criminal Proceedings, The Commonwealth. Available at https://the commonwealth.org accessed December 10

3.4 Commonwealth Models: Indian Evidence Act (1872)

The Commonwealth Model law on electronic evidence is not a single, static law but a collection of various principles and guidelines developed by the Commonwealth Secretariat for member states to legally recognize electronic records, ensuring their admissibility in court by establishing principles for the authenticity, reliability and credibility of such evidence. It focuses on ensuring electronic data(like digital audio, video, computer records) can be trusted and proven in court, supporting the shift to digital economy while tackling cybercrime.[91]

The India Evidence Act (IEA), is a landmark legislation that has served as a foundational "Commonwealth Model" for evidence law across numerous former British colonies and other common law jurisdictions.[92]

The Indian Evidence Act, sections 65A and 65B, establishes specific conditions for the admissibility of electronic records.

These sections mirrored section 5 of the United Kingdom Civil Evidence Act (1968).

The India Evidence Act and the United Kingdom Civil Evidence Act are great influence to other geographical electronic evidence rules like the Nigeria Evidence Act, 2011 (subsequent amendment in 2023).

The Indian Evidence Act and the Evidence Act of Nigeria both originated from Sir James Fitzjames Stephen's *Digest of the law of Evidence*, which serve as a blueprint for codifying evidence law in British colonies.[93]

---

[91] Ibid
[92] The Indian Evidence Act(1872)
[93] Evidence Act, 2011

3.5 Laws and Institutions in Nigeria Regulating Digital Evidence

Nigeria regulates electronic evidence primarily through the Evidence Act, 2011, significantly updated be the Evidence (Amendment) Act,2023, which validates electronic records and digital signatures. Digital evidence are treated as documents for the admissibility under conditions like authentication certificates and experts opinion.

Key national institutions includes, the Judiciary and court(for interpretation and application), the National Information Technology Development Agency (NITDA), Corporate Affairs Commission (CAC), the Economic and Financial Crimes Commission (EFCC) and supported by laws like, the Evidence Act, Cybercrimes Act and the new National Digital Economy and E-Governance Act.

3.5.1 Key Institutions in Nigeria Regulating Digital Evidence

1. The Judiciary and Court: This body interprets and apply the Evidence Act, determine the weight of electronic evidence, and ensure procedural fairness. They serve as key element in the interpretation of the role in which digital evidence play in a court proceeding.

2. The Economic and Financial Crimes Commission (EFCC): They rely on digital tools for data extraction, analyze phone and WhatsApp evidence in high profile cases like (Emiefele's), and conduct large-scale arrests for online fraud, ensuring evidence admissibility through proper procedures and authentication.[94]

3. Central Bank of Nigeria (CBN): This institution regulates electronic banking, dealing with related e-evidence issues, they also keep digital records of any banking transaction,

[94] Sunday, K.A, Appraisal of Electronic Evidence in Nigerian Courts. 20 December,2019. Available at SSRN library, https://papers.ssrn.com, accessed December 10

providing information where needed in cases of financial fraud and laundering.

4. Corporate Affairs Commission: They operate online, uses digital signatures, setting examples for authentication in business.

3.5.2 Key Laws in Nigeria Regulating Digital Evidence

5. Evidence Act 2011(as amended 2023): This is the core legislation, making digital evidence admissible if the conditions established in section 84 are met, including providing a certificate of authentication.

6. Evidence (Amendment) Act 2023: This new Act expanded definitions, recognized digital offenses, ensuring data integrity and security crucial for electronic evidence.[95]

7. National Digital Economy and E-Governance Act 2024: This provides a broad framework for digital transactions and governance, impacting electronic evidence standards.[96]

8. Cybercrimes (Prohibition, Prevention etc) Act,2015: This legislation deals with digital offenses, combats cybercrime and promotes cybersecurity. Protecting private digital information of persons.[97]

The legal system of Nigeria recognizes the significance of digital evidence, hence the creation of laws and institutions to regulate and expand the role of digital evidence and digital records in court proceedings.

[95] Evidence (Amendment) Act 2023
[96] Civil Evidence Act, 1968
[97] Cybercrimes (Prohibition, Prevention etc) Act,2015

The Evidence Act is the foundation of rules governing the admissibility of digital evidence in Nigeria which has aid the development of new laws for the purpose of digital evidence.

3.6 The Impact of International laws on Nigeria Digital Evidence laws

International laws and institutions are great influence on the Nigerian evidence laws. International legal structures established standards to be met for the admissibility and credibility of digital evidence which has been globally recognized and is been integrated into National e-evidence laws.

These notable International evidence law standards integrated into National evidence law, has brought about global alignment and mutual compliance by different geographical jurisdiction.

The Nigeria legal framework for digital evidence was primarily influenced by the Civil Evidence Act, 1968, the Police and Criminal Evidence, 1984 of England (United Kingdom) and the Indian Evidence Act, 1872 (amended 2000).

3.6.1 Influence of the English law (United kingdom)

Nigeria's general law of evidence is deeply rooted in the English legal system due to its colonial history.

The Nigerian Evidence Act, 2011 (and the subsequent 2023 amendment) was influenced by the United Kingdom legislation, such as, the *Civil Evidence Act* and the *Police and Criminal Evidence Act*. The recent provisions of the Evidence Act on digital evidence mirrors the Uk's legislation.

3.6.2 Influence of the Indian Evidence Act

India amended its Evidence Act in 2000 to allow electronic evidence in legal proceedings, a development which occurred before Nigeria's own 2011 amendment. Indian jurisprudence is often referenced in comparative analysis of Nigeria's digital evidence laws.

In the Nigerian Evidence Act, *section 84*, which provides the foundation and procedures for the admissibility of electronic evidence is said to be almost same as *section 65B of the Indian Evidence Act.*

Nigerian courts often look to Indian judicial precedents for guidance on interpreting and applying these provisions, particularly regarding the mandatory requirement for a certificate of authentication which allows for admissibility of digital evidence in any court proceeding.

Major Areas of Influence includes, the shared structure of *section 84* of the *Evidence Act* of Nigeria, which introduced the admissibility of computer-generated and *section 65B of Indian Evidence Act,1872 (as amended 2000)* to allow electronic evidence in legal proceedings.

Section 65B of India Evidence Act provides:[98]

> Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or

[98] *Indian Evidence Act,187*

any contents of the original or of any fact stated therein of which direct evidence would be admissible.

Section 84 of the Evidence Act, provides[99]:

> In any proceedings, 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 the computer in question.

Both sections can be considered to have mirrored each other, for the reason of the admissibility of electronic evidence in a court proceeding. Section 65B of the Indian Evidence Act can be considered to be the birth place of section 84 of the Evidence Act, the requirements to be met for the admissibility of digital evidence established in both subsections are in similar terms and standard.

Another major area of influence is in relation to case laws comparison, Nigeria courts and legal practitioners often look to Indian judicial decisions, such as the *Supreme cou*rt case of *Anvar P.V* v *P.k[100]. Basheer and Arjun Panditrao*, where it was held "*an electronic record by way of secondary evidence shall not be admissible unless the requirement under section 65B are satisfied"*

Also the case of, *Khoktar v Kailash Kushanrao[101]*, where the court held that, *" a certificate under section 65B(4), which verifies the authenticity and integrity of electronic record, is a condition precedent for its admissibility as secondary evidence".*

Both cases are employed for guidance on interpreting the complex conditions for admitting electronic evidence under section 84.

---

[99] *Evidence Act,2011*
[100] (2014),10,SCC,473
[101] AIR 2020 SC 4908, AIRONLINE 2020 SC 641

Lastly, the 2023 Amendment, which further refined rules on electronic records, digital signatures and electronic oath-taking to align with global technological advancements.

3.7 Conclusion

With the influence of International bodies and laws on digital evidence rules in Nigeria, there have been notable advancements and improvements on the requirement of these rules which regulates the admissibility and credibility of digital evidence.

The requirements established by the subsections of 84 of the Evidence Act,2011, have been modernized and redefined under the provisions of the Evidence (Amendment) Act,2023. The new Act established distinct interpretations of various rules regulating digital evidence, interprets the role digital evidence play in a court proceeding, which further aid the judiciary in interpreting and applying digital evidence in a proceeding.

The determination of the admissibility and authentication of digital evidence was historically derived from International legal bodies, the requirements that are to be met by digital evidence before admissibility in Nigeria, is mirrored from various international legal institutions, like the United Kingdom Civil Evidence Act and specifically, the India Evidence Act.

CHAPTER FOUR

ADMISSIBILITY AND CREDIBILITY OF DIGITAL EVIDENCE

4.1 Introduction

The question of whether digital evidence can be admitted in court proceedings has **evolved** from a novel legal issue to a fundamental concern in modern litigation. As our world becomes increasingly digitized, courts face daily challenges with smartphones containing thousands of messages, computer hard drives storing years of documents, and social media accounts chronicling people's lives in unprecedented detail. The challenge isn't whether to admit digital evidence, that debate is over, but rather how to ensure that what enters the courtroom is genuine, reliable, and fair. Digital evidence functions as a double-edged sword. It can provide incredibly detailed and objective records: a text message timestamp showing exactly when someone received information, GPS data revealing a person's location at a critical moment, or surveillance footage capturing an incident as it unfolded.[102] Yet digital evidence is remarkably fragile and malleable. A single keystroke can alter a document, a corrupted file can lose critical information, and sophisticated editing tools can create convincing fabrications.[103]

This chapter explores how courts navigate these complexities when deciding whether to admit digital evidence. When a prosecutor wants to introduce WhatsApp messages in a fraud case, when a civil litigant seeks to admit emails in a breach of contract dispute, or when a party attempts to use social media posts to impeach a witness, judges must apply legal standards developed in an analog world to evidence that exists purely as strings of ones and zeros.

---

[102] Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Academic Press, p. 12.
[103] National Institute of Standards and Technology (2006). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86, p. 2-3. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf Accessed: 9 November 2025.

The Nigerian legal system, like many jurisdictions worldwide, has recognized the inevitability of digital evidence and enacted laws to govern its admissibility. The Evidence Act 2011 marked a turning point, moving Nigeria from outdated colonial-era rules into the digital age.[104] Yet legislation alone cannot answer every question. Courts must still grapple with practical issues: How do we verify that an email actually came from the person it claims to? How can we trust computer-generated logs when we don't understand the underlying software? What happens when crucial evidence sits on servers in another country, subject to different privacy laws?

These aren't merely academic questions. Real cases turn on these issues. A person's freedom may depend on whether their computer files are admitted. A company's survival may hinge on authenticating electronic business records. The stakes are high, and getting the admissibility standards right matters deeply.

4.2 Legal Standards for Admissibility

Understanding the legal standards for digital evidence requires starting with foundational principles that govern all evidence, then examining how these principles apply specifically to electronic materials. Courts don't have entirely separate rules for digital evidence, instead, they adapt existing doctrines to address the unique characteristics of electronic information.

4.2.1 Relevance: The First Hurdle

Every piece of evidence, digital or otherwise, must first be relevant. The evidence must have a logical connection to a fact that matters in the case.[105] Consider a defamation case where the plaintiff wants to introduce tweets from the defendant's account. The tweets are certainly digital evidence, but are they relevant? If they contain the allegedly defamatory statements, absolutely.

---

[104] Evidence Act 2011 (Nigeria), ss. 83-84, 93-94. Available at: https://lawnigeria.com/LawsoftheFederation/EVIDENCE-ACT,-2011.html Accessed: 9 November 2025.
[105] Federal Rules of Evidence (US), Rule 401. Available at: https://www.law.cornell.edu/rules/fre/rule_401 Accessed: 9 November 2025.

But what if they're just other tweets from the same account? The relevance depends on what they're being used to prove, perhaps they establish the defendant's identity as the account holder, or they demonstrate a pattern of behavior.

The Nigerian Evidence Act establishes that evidence is relevant when it relates to facts in issue or is connected to facts in issue.[106] This standard applies equally to digital evidence. In *Buhari v. INEC*, the Supreme Court emphasized that electronic evidence must pass the relevance threshold just like any other evidence, it must help prove or disprove something that actually matters to the case.[107]

4.2.2 Authentication: Proving It Is What You Claim It Is

If relevance is the first hurdle, authentication is often the highest one for digital evidence. Authentication means proving that the evidence is genuine, that it is what its proponent claims it to be. This requirement exists because of a fundamental truth about digital evidence: it's remarkably easy to fake, alter, or misattribute.

Think about an email. When you receive an email that appears to come from john@example.com, how do you really know John sent it? Email protocols make it trivially easy to spoof sender addresses. Courts recognized this problem early on and have developed various methods to authenticate digital evidence.

Direct Evidence Authentication

The simplest way to authenticate digital evidence is through direct testimony from someone with personal knowledge. If John takes the witness stand and testifies, "Yes, I sent that email," and the email is produced, you've authenticated it. Similarly, if the recipient testifies they received the

---

[106] Evidence Act 2011 (Nigeria), s. 1.
[107] *Buhari v. INEC* (2008) 19 NWLR (Pt. 1120) 246 at 340-342. Available at: https://www.lawpavilion.com Accessed: 9 November 2025.

email from John's known email address and the content makes sense in the context of their ongoing communications, courts typically accept this as sufficient authentication.[108]

Circumstantial Evidence and Distinctive Characteristics

More often, digital evidence must be authenticated through circumstantial evidence. Section 84 of the Nigerian Evidence Act provides a framework for this, requiring evidence about how the computer was operating and that the information was supplied in the ordinary course of activities.[109]

Courts look at "distinctive characteristics" to authenticate digital evidence. These might include the sender's known email address or phone number, references to facts only certain people would know, consistency with other authenticated communications, metadata showing creation dates or authors, and patterns of language characteristic of the purported author.[110] The case of *Griffin v. State* illustrates this approach where text messages were admitted based on multiple circumstantial factors including the defendant's phone number, specific relationship details, and consistent communication patterns.[111]

Expert Testimony and Forensic Analysis

For more complex digital evidence, expert testimony often becomes necessary. Digital forensics experts can testify about hash values proving files haven't been altered, metadata analysis revealing document history, recovery of deleted data, and authentication of digital signatures. In *Lorraine v. Markel American Insurance Co.*, Judge Grimm provided comprehensive guidance on

---

[108] *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000). Available at: https://casetext.com/case/united-states-v-siddiqui-15 Accessed: 9 November 2025.
[109] Evidence Act 2011 (Nigeria), s. 84(2).
[110] Federal Rules of Evidence (US), Rule 901(b)(4).
[111] *Griffin v. State*, 19 A.3d 415 (Md. 2011). Available at: https://casetext.com/case/griffin-v-state-390 Accessed: 9 November 2025.

authenticating electronic evidence, noting that experts can help establish the reliability of computer systems, the chain of custody of digital files, and the absence of tampering.[112]

4.2.3 The Hearsay Rule and Its Exceptions

Digital evidence frequently implicates the hearsay rule, which generally excludes out-of-court statements offered to prove the truth of what they assert. A text message saying "John robbed the bank" is hearsay if offered to prove John actually robbed the bank. However, numerous exceptions exist.

The Business Records Exception

This is perhaps the most commonly invoked exception for digital evidence. Section 84 of the Nigerian Evidence Act essentially creates a business records exception for computer-generated evidence, allowing admission of statements in documents produced by computers if foundational requirements are met.[113] The rationale makes sense: businesses rely on their records and have incentives to keep them accurate. However, establishing the foundation requires showing the record was made in the regular course of business, at or near the time of the transaction, by someone with personal knowledge, and that the computer system was functioning properly.

Party Admissions

Statements made by a party to the litigation aren't hearsay when offered against that party. If the defendant posted on Facebook, "I was driving drunk last night," the plaintiff in a civil injury case can introduce that post as a party admission, not hearsay. The challenge comes in proving the

---

[112] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 546 (D. Md. 2007). Available at: https://www.mdd.uscourts.gov/ Accessed: 9 November 2025.
[113] Evidence Act 2011 (Nigeria), s. 84(1).

party actually made the statement, accounts get hacked, friends post on each other's pages, and identities get stolen.[114]

Present Sense Impressions and Excited Utterances

These traditional hearsay exceptions have found new life in the digital age. A text message sent during an event describing what's happening might qualify as a present sense impression. A WhatsApp voice message sent immediately after a traumatic event, where the speaker is clearly under stress, might be an excited utterance. The timestamp on a message can help establish it was sent during or immediately after an event.[115]

4.2.4 The Best Evidence Rule

Traditionally, the best evidence rule required production of original documents rather than copies. This rule has been significantly modified for digital evidence because the concept of an "original" becomes murky in the electronic context. Is the "original" email the version on the sender's server, the recipient's computer, or the backup tape? Section 83 of the Nigerian Evidence Act addresses this by allowing proof of documents through authenticated copies, effectively recognizing that for electronic evidence, a properly authenticated copy is as good as an original.[116]

4.2.5 The Certificate Requirement Under Nigerian Law

---

[114] *Commonwealth v. Williams*, 456 Mass. 857, 926 N.E.2d 1162 (2010). Available at: https://caselaw.findlaw.com/ma-supreme-judicial-court/1532574.html Accessed: 9 November 2025.
[115] Shearing, V. and Macaulay, R. (2020). 'Text Messages as Evidence', *Journal of Digital Forensics, Security and Law*, 15(2), pp. 95-112.
[116] Evidence Act 2011 (Nigeria), s. 83.

Section 84(4) of the Nigerian Evidence Act introduces a unique requirement: computer-generated evidence must generally be accompanied by a certificate identifying the document, describing how it was produced, and providing details about the device involved.[117] This certificate must be signed by a person occupying a responsible position in relation to the computer's operation.

In *Dickson v. Sylva*, the Court of Appeal strictly applied this provision, holding that without proper certification, computer-generated evidence should not be admitted.[118] The court reasoned that the certificate serves as a safeguard, ensuring the party offering the evidence has properly verified its source and reliability. However, critics argue this requirement is overly rigid and may exclude otherwise reliable evidence on technicalities.

4.2.6 Technical Requirements

Beyond the legal standards, digital evidence must meet certain technical requirements to be admissible. These requirements ensure the evidence is reliable, hasn't been tampered with, and can be meaningfully presented to the court.

4.2.7 Chain of Custody: Tracking Evidence from Collection to Courtroom

The chain of custody represents perhaps the most critical technical requirement for digital evidence. It's the documented chronology showing who handled the evidence, when they handled it, and what they did with it.[119] For digital evidence, this is complex because digital data is inherently volatile, unlike a gun that sits unchanged in an evidence locker, digital files can be modified, corrupted, or destroyed through normal computer operations.

---

[117] Evidence Act 2011 (Nigeria), s. 84(4).
[118] *Dickson v. Sylva* (2015) LPELR-24503(CA). Available at: https://www.lawpavilion.com Accessed: 9 November 2025.
[119] Mohay, G. et al. (2003). *Computer and Intrusion Forensics*. Artech House, pp. 89-95.

Initial Collection and Seizure

The chain of custody begins at collection. When law enforcement seizes a computer, tablet, or phone, proper procedure involves photographing the device and its surroundings, documenting the device's state, preventing remote wiping using Faraday bags, properly packaging and labeling the device, and creating detailed notes about the collection process.[120] In *State v. Cook*, the court excluded digital evidence where law enforcement failed to properly document the collection process and couldn't prove the device hadn't been accessed between seizure and analysis.[121]

Forensic Imaging

Rather than working with original devices, digital forensic examiners create forensic images, exact bit-by-bit copies of storage media. This process involves write-blocking to prevent any writing to the original device, creating a duplicate copy of every bit of data, generating a cryptographic hash value that acts as a unique digital fingerprint, and verifying the duplicate's hash matches the original's hash.[122] The hash values are crucial, if examined again months later, new hash values can be calculated and compared to the originals. If they match, nothing has changed.

4.2.8 Data Integrity and Verification

Beyond chain of custody, courts must be satisfied that digital evidence hasn't been altered, corrupted, or tampered with.

Hash Values and Digital Fingerprints

---

[120] NIST (2006). *Guide to Integrating Forensic Techniques*, pp. 3-5 to 3-8.
[121] *State v. Cook*, 145 Wash. App. 784, 187 P.3d 1151 (2008). Available at: https://caselaw.findlaw.com/wa-court-of-appeals/1432878.html Accessed: 9 November 2025.
[122] Casey, E. (2011). *Digital Evidence and Computer Crime*, pp. 45-52.

Hash functions create unique values from data, like digital fingerprints. Even changing a single character in a document produces a completely different hash value. This makes hashes incredibly useful for verifying integrity. This dramatic change from tiny alterations makes hashes ideal for detecting tampering.[123]

Metadata Examination

Metadata, data about data, can reveal crucial information about digital evidence's integrity. File metadata typically includes creation date and time, last modification date and time, last access date, author information, software used to create the file, and edit history.[124] However, metadata can be manipulated, so experts need to examine it carefully for signs of tampering.

4.2.9 Technical Standards and Best Practices

Various organizations have developed technical standards for handling digital evidence. While not legally binding, these standards influence what courts consider acceptable practice.

The International Organization on Computer Evidence (IOCE) established six fundamental principles, including that actions taken shouldn't change evidence, examiners must be competent, an audit trail should be created and preserved, and documentation should allow independent reconstruction.[125] The Scientific Working Group on Digital Evidence (SWGDE) has published best practices covering evidence collection, examination, and reporting.[126]

---

[123] *United States v. Bansal*, 663 F.3d 634 (3d Cir. 2011). Available at: https://casetext.com/case/united-states-v-bansal-3 Accessed: 9 November 2025.
[124] Garrie, D.B. and Gelb, M. (2007). *E-Discovery & Digital Evidence*. Thomson West, pp. 234-240
[125] International Organization on Computer Evidence (2000). *Guidelines for Best Practice in the Forensic Examination of Digital Technology*.
[126] Scientific Working Group on Digital Evidence (2016). *SWGDE Best Practices for Computer Forensics*. Available at: https://drive.google.com/file/d/1M_OWBlF5fikNH2BREaoBoHKlRF0L0N5i/view Accessed: 9 November 2025.

Nigerian courts have begun referencing these international standards. In *Federal Republic of Nigeria v. Ogbonna*, the trial court noted that the prosecution's digital forensic examiner had followed SWGDE guidelines, lending credibility to his testimony about proper handling procedures.[127]

4.2.10 Technical Competence and Expert Qualifications

The technical requirements for digital evidence necessarily implicate questions about who should handle such evidence and what qualifications they need. While no universal licensing requirement exists for digital forensic examiners, various certifications have emerged including Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE), and GIAC Certified Forensic Analyst (GCFA).[128]

The U.S. Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals* established factors for evaluating expert testimony, including the expert's qualifications and whether their methods have been peer-reviewed and generally accepted in the relevant scientific community.[129] These factors apply equally to digital forensic experts.

4.2.11 Jurisdictional Variations

While fundamental principles of evidence law remain relatively consistent across jurisdictions, significant variations exist in how different legal systems approach digital evidence admissibility.

4.2.12 The Nigerian Approach

---

[127] *Federal Republic of Nigeria v. Ogbonna* (2019) LPELR-46234(CA). Available at: https://www.lawpavilion.com Accessed: 9 November 2025.
[128] Casey, E. (2011). *Digital Evidence and Computer Crime*, pp. 567-570.
[129] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993). Available at: https://supreme.justia.com/cases/federal/us/509/579/ Accessed: 9 November 2025.

Nigeria's Evidence Act 2011 represents a comprehensive legislative response to digital evidence, but Nigerian courts have interpreted these provisions in ways that create unique characteristics. The certificate requirement under Section 84(4) is more stringent than in many other jurisdictions and has generated substantial case law. In *Dickson v. Sylva*, the Court of Appeal set a high bar, requiring strict compliance with the certification requirements.[130] This strict interpretation has been criticized for potentially excluding reliable evidence on technicalities, though defenders argue it ensures proper verification and prevents sloppy evidence handling.

Nigerian courts retain significant discretion in admissibility determinations despite the statutory framework. In *APC v. INEC*, the Court of Appeal admitted WhatsApp messages and social media posts in an election petition, taking a relatively flexible approach to authentication and certification requirements.[131] This flexibility has created some uncertainty about when courts will strictly enforce technical requirements versus when they'll take a more pragmatic approach.

4.2.13 The United States Federal System

The U.S. approach to digital evidence provides interesting contrasts with Nigeria's system, particularly in its emphasis on flexible standards rather than rigid certification requirements. Federal Rule of Evidence 901 requires authentication but doesn't mandate specific methods, giving courts flexibility to accept various forms of proof.[132] For example, in *United States v. Hassan*, the Fourth Circuit admitted Facebook messages based on circumstantial evidence including the account's profile information and testimony from a recipient who had communicated with that account.[133] Certain types of evidence can be self-authenticating under Federal Rule of Evidence 902. Rules 902(13) and (14), added in 2017, allow self-authentication

[130] *Dickson v. Sylva* (2015) LPELR-24503(CA).
[131] *APC v. INEC* (2020) LPELR-49567(CA). Available at: https://www.lawpavilion.com Accessed: 9 November 2025.
[132] Federal Rules of Evidence (US), Rule 901.
[133] *United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014). Available at: https://casetext.com/case/united-states-v-hassan-55 Accessed: 9 November 2025.

of records generated by electronic processes or systems that produce accurate results, provided the proponent certifies the process used and gives advance notice to opponents.[134]

4.2.14 The United Kingdom and Commonwealth Approaches

The UK's Police and Criminal Evidence Act 1984 originally included Section 69, which required specific proof that computers were operating properly before computer-generated evidence could be admitted. This proved burdensome in practice and Section 69 was abolished by the Youth Justice and Criminal Evidence Act 1999, moving to a presumption that computers were operating properly unless there was evidence to the contrary.[135]

The UK treats digital evidence somewhat differently in civil versus criminal proceedings. The Civil Evidence Act 1995 abolished the hearsay rule in civil cases, making it much easier to admit digital evidence without navigating complex hearsay exceptions.[136] Criminal cases retain more restrictions, though the Criminal Justice Act 2003 substantially liberalized hearsay rules there as well.

4.2.15 Cross-Border Evidence Issues

Perhaps the most challenging jurisdictional issues arise when digital evidence spans borders, which increasingly occurs as data migrates to cloud servers located anywhere globally. When evidence is located in another country, law enforcement typically must use Mutual Legal Assistance Treaties (MLATs) to request assistance from foreign authorities. This process can be slow and cumbersome, sometimes taking years to complete.[137]

---

[134] Federal Rules of Evidence (US), Rules 902(13)-(14) (2017 amendments).
[135] Youth Justice and Criminal Evidence Act 1999 (UK), c. 23, s. 60, Sch. 3. Available at: https://www.legislation.gov.uk/ukpga/1999/23/contents Accessed: 9 November 2025.
[136] Civil Evidence Act 1995 (UK), c. 38. Available at: https://www.legislation.gov.uk/ukpga/1995/38/contents Accessed: 9 November 2025.
[137] Gercke, M. (2012). *Understanding Cybercrime*. International Telecommunication Union, pp. 245-267.

The Budapest Convention on Cybercrime attempts to streamline cross-border cooperation by establishing common standards and expedited procedures for obtaining digital evidence across borders.[138] Nigeria has not yet ratified the Budapest Convention, though regional instruments like the African Union Convention on Cyber Security and Personal Data Protection aim to facilitate intra-African cooperation.

4.2.16 Challenges in Admissibility

Even when digital evidence theoretically meets legal and technical requirements, practical challenges often arise in getting it admitted.

4.2.17 The Technical Knowledge Gap

Perhaps the most significant challenge is the technical knowledge gap between legal professionals and digital technologies. Most judges, lawyers, and even jurors lack deep understanding of how computers, networks, and digital forensics actually work.[139] When a digital forensic expert testifies about hash values, encryption algorithms, and metadata parsing, judges must understand enough to make informed rulings about admissibility.

This knowledge gap can lead to accepting unreliable evidence because technical flaws aren't recognized, excluding reliable evidence due to misunderstanding legitimate technical limitations, or inability to effectively question expert witnesses.[140] Some jurisdictions have implemented judicial education programs on digital evidence to address this gap.

4.2.18 Authentication Challenges for Specific Evidence Types

---

[138]Council of Europe Convention on Cybercrime, 23 November 2001, ETS No. 185, Arts. 23-35. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention Accessed: 9 November 2025.
[139] Mnookin, J.L. (2001). 'Scripting Expertise', *Virginia Law Review*, 87(8), pp. 1723-1845.
[140] Lederer, F.I. (2005). 'The Road to the Virtual Courtroom', *South Carolina Law Review*, 50, pp. 799-855.

Different types of digital evidence present unique authentication challenges that can complicate admissibility.

Social Media Evidence

Social media posts raise thorny authentication questions. Just because content appears on someone's Facebook page doesn't mean they posted it, accounts get hacked, friends post on each other's timelines, and profile information can be falsified. In *Commonwealth v. Williams*, the Massachusetts Supreme Judicial Court held that screenshots of Facebook messages required more than just showing the profile name matched the defendant, additional circumstantial evidence was needed.[141]

Text Messages and Encrypted Communications

Text messages and encrypted messaging apps like WhatsApp present similar problems. Phone numbers can be spoofed and messages can be fabricated. Courts typically require more than just showing a message came from a particular phone number, additional authentication might include testimony from the recipient about prior communications, distinctive content revealing the sender's identity, or expert testimony about metadata.[142]

Digital Images and Videos: The Deepfake Problem

Advances in artificial intelligence and image manipulation software have shattered the assumption that "seeing is believing." Deepfakes, AI-generated fake videos and images, can convincingly depict events that never occurred.[143] Some courts have begun requiring enhanced authentication for digital images and videos, including expert testimony about

---

[141] *Commonwealth v. Williams*, 456 Mass. 857, 926 N.E.2d 1162 (2010).
[142] *Griffin v. State*, 19 A.3d 415 (Md. 2011).
[143] Chesney, R. and Citron, D.K. (2019). 'Deep Fakes', *California Law Review*, 107(6), pp. 1753-1820. Available at: https://www.californialawreview.org/ Accessed: 9 November 2025.

Forensic Analysis for Signs of Manipulation

Cryptocurrency and Blockchain Evidence

Cryptocurrency transactions present novel authentication challenges. While blockchain records are theoretically immutable and transparent, proving who actually controlled a particular wallet address at a specific time can be difficult because cryptocurrency transactions are pseudonymous, tied to wallet addresses rather than real identities.[144]

4.2.19 Preservation and Spoliation Issues

Digital evidence is fragile. Once litigation is reasonably anticipated, parties have a duty to preserve relevant evidence, including digital evidence. This duty can be extensive, requiring preservation of emails, documents, databases, and even metadata.[145] When digital evidence is lost or destroyed, courts may exclude other evidence, give adverse inference instructions, dismiss claims, or award monetary sanctions. Courts generally distinguish between negligent loss and intentional destruction, with intentional spoliation receiving harsher treatment.[146]

4.2.20 Cost and Complexity

The cost and complexity of properly collecting, preserving, and presenting digital evidence can create admissibility challenges, particularly for less-resourced parties. Professional digital forensic services are expensive, a comprehensive forensic examination of a single computer can

---

[144] *Tulip Trading Ltd v. Bitcoin Association* [2022] EWHC 141 (Ch). Available at: https://www.bailii.org/ew/cases/EWHC/Ch/2022/141.html Accessed: 9 November 2025.
[145] *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003). Available at: https://casetext.com/case/zubulake-v-ubs-warburg-llc-6 Accessed: 9 November 2025.
[146] Federal Rules of Civil Procedure (US), Rule 37(e). Available at: https://www.law.cornell.edu/rules/frcp/rule_37 Accessed: 9 November 2025.

cost thousands of dollars.[147] This creates justice concerns, as well-resourced parties can afford comprehensive forensic services while individuals or indigent defendants may struggle.

Modern litigation often involves massive volumes of digital evidence. A single executive's email archive might contain hundreds of thousands of messages. Reviewing this material to determine what's relevant and admissible is enormously time-consuming and expensive. Predictive coding and technology-assisted review tools can help manage volume, but they introduce new admissibility questions.[148]

4.2.21 Privacy and Privilege Concerns

Digital evidence collection often implicates privacy rights and legal privileges in ways that physical evidence typically doesn't. Smartphones and computers contain vast amounts of personal information, and Section 37 of the Nigerian Constitution protects privacy of citizens.[149] Courts must balance this constitutional protection against law enforcement needs and litigants' rights to discover relevant evidence.

Digital devices and accounts may contain privileged communications between lawyers and clients. When investigators image a computer or examine email accounts, they might inadvertently access privileged materials, leading to waiver arguments and admissibility disputes.[150]

4.2.22 Rapid Technological Change

---

[147] Scheindlin, S.A. and Rabkin, J. (2004). 'Electronic Discovery in Federal Civil Litigation', *New York University Journal of Law and Liberty*, 4, pp. 88-125.
[148] *Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y. 2012). Available at: https://casetext.com/case/da-silva-moore-v-publicis-groupe Accessed: 9 November 2025.
[149] Constitution of the Federal Republic of Nigeria 1999 (as amended), s. 37. Available at: https://www.wipo.int/edocs/lexdocs/laws/en/ng/ng014en.pdf Accessed: 9 November 2025.
[150] *In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003). Available at: https://casetext.com/case/in-re-ford-motor-co-6 Accessed: 9 November 2025.

Perhaps the most fundamental challenge is that technology evolves faster than law can adapt. Consider the evolution just in the past fifteen years: smartphones with enormous storage capacity, cloud computing dispersing data globally, end-to-end encrypted messaging, cryptocurrency and blockchain, Internet of Things devices, artificial intelligence, and quantum computing threatening current encryption.[151]

Each innovation creates new evidentiary questions. Courts applying decades-old evidence rules to cutting-edge technology face an inherent mismatch. While fundamental principles remain sound, their application must be flexible enough to accommodate technologies that didn't exist when the rules were written.

4.2.23 Case Studies and Judicial Precedents

Examining specific cases provides concrete illustrations of how courts have addressed digital evidence admissibility challenges.

4.2.24 Nigerian Cases

Buhari v. INEC (2008)

This landmark case arose from Nigeria's 2007 presidential election. The petitioners sought to introduce electronic evidence including computer printouts, but the Supreme Court engaged with the requirements of Section 83-84 of the then-applicable Evidence Act. While the Court ultimately did not admit much of the electronic evidence due to failure to meet statutory requirements, the case established important precedents: electronic evidence must meet the same

[151] Kerr, O.S. (2004). 'The Fourth Amendment and New Technologies', *Michigan Law Review*, 102(5), pp. 801-888. Available at: https://repository.law.umich.edu/mlr/ Accessed: 9 November 2025.

relevance standards as traditional evidence, proper authentication is essential, and parties must understand and comply with statutory requirements.[152]

[152] (2008) NWLR (Pt. 1120) 246.

Dickson v. Sylva (2015)

This Court of Appeal decision strictly interpreted the certificate requirement under Section 84(4). The appellant sought to introduce text messages and call logs, but the court found the certification inadequate. The court held that the certificate must specifically identify the document, describe how it was produced, and provide detailed particulars about the device used.[153]

APC v. INEC (2020)

In this election petition, the Court of Appeal took a more flexible approach, admitting WhatsApp messages and social media posts. The court recognized the practical difficulties of obtaining perfect certification for social media content while emphasizing the need for adequate authentication through circumstantial evidence.[154]

4.2.25 United States Cases

Lorraine v. Markel American Insurance Co. (2007)

Judge Grimm's opinion has become perhaps the most influential U.S. decision on electronic evidence admissibility, providing comprehensive analysis of authentication, hearsay, and best evidence rule issues. Key holdings included that electronic evidence must be authenticated through sufficient evidence, the same hearsay exceptions apply to electronic documents, and the best evidence rule doesn't require production of the original computer.[155]

---

[153] (2015) LPELR-24503(CA).
[154] *APC v. INEC* (2020) LPELR-49567(CA).
[155] *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007).

United States v. Vayner (2014)

This case addressed authentication of social media evidence in criminal prosecution. The defendant was charged with threatening federal officials through Facebook messages. The Seventh Circuit required additional circumstantial evidence beyond just the Facebook profile name, including evidence that the defendant accessed the account and information in the messages that only the defendant would know.[156]

Riley v. California (2014)

While primarily a Fourth Amendment case about warrantless cell phone searches, *Riley* has significant implications for digital evidence admissibility. The Supreme Court's holding that warrantless cell phone searches incident to arrest are unconstitutional affects evidence admissibility, evidence obtained in violation of *Riley* may be excluded under the exclusionary rule.[157]

4.2.26 United Kingdom Cases

R v. Cochrane (1993)

This Court of Appeal case addressed admissibility of electronic till receipts. The court established that the party opposing admission bore the burden of showing the computer wasn't functioning properly, rather than the proponent having to affirmatively prove proper functioning

[156] *United States v. Vayner*, 769 F.3d 125 (2d Cir. 2014). Available at: https://casetext.com/case/united-states-v-vayner-1 Accessed: 9 November 2025.
[157] *Riley v. California*, 573 U.S. 373 (2014). Available at: https://supreme.justia.com/cases/federal/us/573/373/ Accessed: 9 November 2025.

in every detail. This presumption of proper functioning has been influential in Commonwealth jurisdictions.[158]

Tulip Trading Ltd v. Bitcoin Association (2022)

This recent case involved blockchain evidence in a dispute over cryptocurrency ownership. The High Court recognized blockchain's theoretical immutability and transparency as factors supporting reliability, but also acknowledged practical challenges in authenticating who controlled particular wallet addresses.[159]

4.2.27 Comparative Analysis of Key Precedents

Looking across these cases, several themes emerge. Courts constantly balance between flexibility (accommodating new technology and practical realities) and rigor (maintaining standards that ensure reliability). Virtually every significant digital evidence case grapples with authentication, as digital evidence requires understanding technical systems and trust in processes.

Expert testimony features prominently in digital evidence cases, and courts have become more discerning about expert qualifications and methodologies. Cases like *Riley* demonstrate judicial awareness that digital evidence implicates fundamental rights in ways physical evidence often doesn't, and courts are developing frameworks for balancing investigative needs against privacy protections.[160]

---

[158] *R v. Cochrane* [1993] Crim LR 48 (CA). Available at: https://www.lexisnexis.co.uk/legal/ Accessed: 9 November 2025.
[159] *Tulip Trading Ltd v. Bitcoin Association* [2022] EWHC 141 (Ch).
[160] *Riley v. California*, 573 U.S. 373 (2014)

4.2.28 Conclusion

The admissibility of digital evidence represents one of the most dynamic areas of modern evidence law. Courts worldwide are adapting traditional evidence principles to accommodate digital realities while maintaining appropriate safeguards for reliability and fairness.

The legal standards, relevance, authentication, hearsay exceptions, and best evidence considerations, remain fundamentally sound. However, their application to digital evidence requires technical understanding and flexibility that courts are still developing. Technical requirements around chain of custody, data integrity, and forensic methodology have become equally important, yet many legal professionals lack adequate technical training.

Jurisdictional variations reflect different policy choices. Nigeria's certificate requirement provides certainty but may be overly rigid, while U.S. flexibility accommodates new technologies but may sometimes sacrifice thoroughness. Finding the right balance remains an ongoing challenge.

The practical challenges are substantial: technical knowledge gaps, authentication difficulties, preservation issues, costs, privacy concerns, and rapid technological change. These challenges won't disappear, technology will continue evolving, and law will continue adapting.

The case law demonstrates both progress and persistent uncertainties. Courts have become more sophisticated in handling digital evidence, yet each new technology presents fresh questions. Looking forward, likely developments include increased judicial education on technical issues, greater harmonization of standards across jurisdictions, development of specialized expertise, continued evolution of forensic techniques, and new legislation addressing emerging technologies.

What remains constant is the fundamental purpose of evidence law: to facilitate accurate fact-finding while protecting rights and ensuring fairness. Whether the evidence arrives on paper or pixels, these principles endure.

4.3 Introduction to Credibility of Digital Evidence

Nigerian courts today are dealing with an increasing volume of digital evidence in criminal cases. From fraud prosecutions to cybercrime investigations, electronic records have become central to proving or disproving allegations.[161] However, digital evidence brings unique problems that traditional physical evidence does not present. A document can be examined for signs of physical tampering - erasures, alterations, or forgery marks. But digital files can be modified without leaving any visible trace to the untrained eye.

This volatility of digital evidence makes it particularly vulnerable. Someone can delete thousands of files with a single click. A sophisticated user can alter timestamps, edit documents, or even create entirely fabricated electronic records that appear authentic.[162] These characteristics demand that courts approach digital evidence with particular caution and insist on proper authentication before admitting it.

The Evidence Act 2011 provides the primary legal framework governing admissibility of evidence in Nigeria, including electronic evidence.[163] Section 84 of the Act specifically addresses the admissibility of computer-generated evidence, providing that statements contained in documents produced by computers shall be admissible as evidence of facts stated therein,

---

[161] G Obamanu, 'Legal Issues and Challenges in the Admissibility of Digital Forensic Evidence in Courts in Nigeria' (2023) 8(01) AJIEEL 96

[162] Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn, Academic Press 2011) 12.

[163] Evidence Act 2011 (as amended).

subject to certain conditions being satisfied.[164] But the Act was drafted in an era when digital evidence was less prevalent than it is today. Courts must therefore interpret these provisions in light of technological realities that the drafters may not have fully anticipated. Evidence that fails to meet the Act's requirements for authenticity and reliability cannot be admitted, regardless of how probative it might appear.

This chapter examines how digital evidence is authenticated and evaluated in Nigerian courts. It discusses the factors affecting credibility, the technical mechanisms used to verify authenticity, and the practical challenges that arise when presenting electronic evidence in legal proceedings.

4.3.1 Factors Affecting Credibility of Digital Evidence

Courts evaluating digital evidence must consider three fundamental questions: Is this evidence authentic? Is it reliable? Has it been properly handled from collection to presentation? These questions are not unique to digital evidence, but answering them requires different approaches than traditional evidence demands.[165] Authenticity means proving that the evidence is genuinely what it claims to be. When a prosecutor presents an email allegedly sent by the accused, the court must be satisfied that this email was actually sent by that person and not fabricated or sent by someone else using their account. With digital evidence, establishing authenticity often requires technical analysis rather than simple visual inspection.[166]

Reliability addresses whether the evidence accurately represents the facts and whether proper methods were used to collect and analyze it. A poorly conducted forensic examination might

---

[164] *Ibid*, s 84.
[165] [2010] EWCA Crim 1859, [35].
[166] S Mason , *Electronic Evidence* (4th edn, LexisNexis 2017) 45-48.

miss crucial evidence or, worse, produce misleading results. Courts therefore need assurance that investigators followed sound procedures and used appropriate tools.

The chain of custody becomes especially critical with digital evidence because of how easily it can be altered. Unlike a physical document that can be sealed in an evidence bag, digital evidence often must be copied multiple times - for analysis, for sharing with other investigators, for providing to defense counsel.[167] Each copy creates a potential point where tampering could occur. Comprehensive documentation showing every person who handled the evidence, what they did with it, and when they did it becomes essential for proving the evidence remains uncompromised.

Beyond these foundational issues, several specific challenges affect how Nigerian courts evaluate digital evidence. Understanding these challenges helps explain why certain authentication procedures are necessary.

4.3.2 Data Fragmentation and Integration Problems

One practical difficulty investigators face is that digital evidence often exists in fragmented form across multiple systems. In a fraud investigation, for instance, relevant evidence might include bank records in one system, email communications in another, phone records from telecommunications providers, and social media activity on various platforms. Each system stores data differently and may not communicate with the others.

This fragmentation creates real problems for investigations. Manually transferring data between systems invites errors and may lose important contextual information. More critically for court

[167] National Institute of Standards and Technology (NIST), *Guidelines on Mobile Device Forensics* (2014) SP 800-101 Rev 1, 23.

proceedings, when evidence exists in disconnected silos, maintaining a clear chain of custody becomes extremely difficult. How do you prove that evidence was not altered when it passed through multiple hands and multiple systems, each with different security protocols and logging capabilities?

The lack of integrated systems also limits what investigators can discover. Modern analytical tools can identify patterns and connections across large datasets, but they need access to consolidated information to work effectively. When data remains scattered in incompatible systems, these powerful capabilities cannot be fully utilized.[168]

4.3.3 Vulnerability to Tampering and Cyber Attacks

Digital evidence can be altered in seconds, and sophisticated alterations may leave no obvious traces.[169] This makes it fundamentally different from physical evidence. Someone trying to forge a paper document must physically alter it in ways that forensic examination can usually detect. But editing a digital file can be done seamlessly with readily available software.

The threat is not just from deliberate tampering by suspects. Malware can corrupt files. Ransomware can encrypt evidence, potentially destroying it if the ransom is not paid. Unauthorized access to systems storing evidence creates opportunities for modification or theft. These cybersecurity threats have become increasingly sophisticated, and investigators must constantly update their defenses.

Protecting digital evidence requires multiple layers of security. Access controls should limit who can view or modify evidence. Encryption protects data both when stored and when transmitted.

[168] Malik Hamad Al-Mashagbeh and others, 'Investigators of Digital Evidence: Main Challenges and Solutions' (2024) International Journal of Information Security available at www.researchgate.net accessed 20 November 2025.
[169] Sammons J, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* (2nd edn, Syngress 2014) 67.

Detailed audit logs automatically record every access to evidence, creating a trail that can reveal unauthorized activity. Regular backups stored in secure locations protect against both accidental and deliberate destruction.

But technology alone is insufficient. Investigators must follow standardized procedures that courts recognize as reliable. Proper documentation, rigorous chain of custody protocols, and validated forensic techniques all contribute to demonstrating that evidence has not been compromised.[170]

4.3.4 Diversity of Devices and Formats

Walk into any Nigerian office or home and you will find an array of digital devices: smartphones, computers, tablets, perhaps smart watches or IoT devices. Each operates differently, stores data in its own format, and requires specific expertise to examine properly. A forensic examiner expert in analyzing Windows computers may struggle with iOS devices, and vice versa.

This diversity creates practical problems for investigators. They must maintain expertise across multiple platforms and constantly update their skills as new devices and operating systems appear.[171] The tools that work for one type of device may be useless for another. Even within a single device type, different models or software versions may store data differently.

For courts, this complexity means that establishing the reliability of forensic methods becomes more challenging. An examiner may use well-established techniques for one type of device but need to employ novel methods for newer technology. Defense counsel can then challenge whether these newer methods have been sufficiently validated.

---

[170] Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence* (Version 5, 2012) 6-8.
[171] Al-Zarouni M, 'Mobile Handset Forensics: An Overview' (2006) 3(2) International Journal of Digital Evidence 1, 3.

4.3.5 Human Error in Evidence Handling

Technology provides tools for preserving and analyzing evidence, but humans must use those tools properly. Mistakes during evidence collection, preservation, or analysis can compromise even the most advanced technical safeguards.

An investigator who fails to use write-blocking when imaging a hard drive may inadvertently modify data on the original device. Someone who stores evidence on media that is not write-protected risks accidental modification during later access. Improper environmental storage can cause data degradation. Even connecting an evidence device to the wrong analysis system might introduce malware or cause unintended changes.

Errors during analysis can be equally problematic. Misinterpreting forensic tool outputs, using inappropriate analytical methods, or failing to validate findings before reporting them can all lead to flawed conclusions. And presentation errors, though perhaps less technically serious, can cause judges or jurors to misunderstand crucial evidence.

Reducing human error requires comprehensive training, clear standardized procedures, and effective quality control.[172] Peer review processes where a second examiner independently verifies findings can catch mistakes before they affect cases. Regular proficiency testing identifies personnel who need additional training. Case audits help identify recurring problems that should be addressed systemically.

Creating a culture where people feel comfortable reporting errors rather than hiding them is equally important. When mistakes are discovered early, their impact can often be minimized. But

[172] *Ibid*, note 10, 12.

if fear of punishment causes people to conceal errors, problems may only surface at trial, where they can devastate the prosecution's case.

4.3.6 Risks during Evidence Transfer

Digital evidence frequently must be shared among multiple parties. Investigators may need to send evidence to forensic laboratories for analysis. Prosecutors need access to prepare for trial. Defense counsel must receive copies for their own examination. Courts may require evidence for review. Each transfer creates security risks.

Network transmission exposes evidence to potential interception or modification. Physical transport of storage media creates risks of loss, theft, or damage. Without proper verification procedures, evidence might be sent to wrong recipients or intercepted en route. Incompatible systems or file formats can cause corruption during transfer even when no malicious activity occurs.

Secure transfer protocols become essential. Encryption protects data during transmission. Strong authentication verifies the identities of both senders and recipients.[173] Detailed documentation tracks every transfer, recording who sent what evidence to whom and when. Recipients should confirm receipt and verify that what they received matches what was sent.

The chain of custody must extend to all transfers. Each time evidence moves from one custodian to another, that movement must be documented with sufficient detail to prove the evidence remained properly controlled.

4.3.7 Authentication Mechanisms

[173] Scientific Working Group on Digital Evidence (SWGDE), *Best Practices for Computer Forensics* (Version 3.1, 2014) 8.

In the digital age, where information is readily accessible and easily replicated, the authentication of digital evidence is crucial for ensuring its reliability and admissibility in legal proceedings. Authentication refers to the process of establishing the authenticity and genuineness of digital data, confirming that it has not been tampered with or altered. This document explores key aspects of digital evidence authentication, encompassing legal admissibility, forensic techniques, and the challenges associated with establishing its validity.

4.3.8 The Daubert Standard

The Daubert Standard, set by the 1993 Daubert v. Merrell Dow Pharmaceuticals case, outlines the criteria for allowing scientific evidence in federal courts. To be admissible, evidence must be scientifically valid, meaning it's testable, has undergone peer review, and is widely accepted in the scientific community. Digital evidence, such as electronic files or communications, must meet these standards. For instance, forensic analysis of a computer may be allowed if the methods are sound, validated, and accepted by experts. The court considers factors like methodology, analyst qualifications, and reliability of the software or tools used in the analysis.[174]

[174] 509 US 579 (1993).

4.3.9 The Frye Standard

The Frye Standard, set by the 1923 *Frye v. United States* case, is a common criterion for admitting scientific evidence. It requires that the evidence be widely accepted by the relevant scientific community, meaning the methods used must be recognized and trusted by experts. For example, digital fingerprint analysis may be allowed under Frye if forensic experts broadly accept the techniques. The court assesses the technique's acceptance, software reliability, and analyst qualifications.[175]

4.3.10 Forensic Imaging

Forensic imaging is a crucial step in authenticating digital evidence, ensuring data is preserved and its integrity is maintained. It creates a precise, bit-by-bit copy of the original digital source, such as a hard drive or mobile device, without changing the original data. This forensic image is an exact duplicate, capturing every detail. By doing so, forensic imaging ensures the evidence remains unchanged during investigation, preventing any unintentional or deliberate alterations that could undermine its validity.

4.3.11 Hashing

Hashing is key to authenticating digital evidence, creating a unique digital identifier for the data. A hash function, a mathematical algorithm, converts input data into a fixed-length string of characters, or hash value, acting as a digital signature. This hash value is unique to the original data, and any alteration, no matter how small, changes the hash. This makes hashing a powerful tool for confirming data integrity and spotting any tampering.

---

[175] 293 F. 1013 (D.C. Cir. 1923).

4.3.12 Chain of Custody

Establishing a chain of custody is a critical part of authenticating digital evidence, involving a detailed record of how and where the evidence was handled from collection to court presentation. This thorough documentation maintains evidence integrity and authenticity by preventing unauthorized access, tampering, or changes. The chain must be continuous, documenting every transfer with dates, times, and handlers' names. This meticulous record proves the evidence was unaltered and its integrity preserved. For example, seizing a digital file involves documenting every step - from law enforcement collection to lab transfer, including times, dates, handlers, and procedures. This ensures evidence admissibility in court, confirming proper handling and uncompromised authenticity.

4.3.13 Documentation

Thorough documentation is crucial for supporting the chain of custody and authenticating digital evidence, covering collection, analysis, and changes made. It includes detailed notes, reports, and logs outlining investigation steps, tools used, and findings. This comprehensive record provides a clear account of evidence handling, making it verifiable. A forensic report, for instance, should detail methods, software, and results, plus any evidence alterations and reasons. This transparency ensures evidence admissibility in court and allows verification by legal and independent experts.

4.3.14 Metadata

Metadata refers to data about data. It provides information about the characteristics of a digital file, such as its creation date, modification date, author, file size, and file type. Metadata can be crucial for authenticating digital evidence, as it offers insights into the origin, history, and

potential alterations of a file. For instance, if a file's creation date differs significantly from the date it was allegedly created, it could raise suspicion about its authenticity. Examining metadata can reveal potential tampering, provide context for the file's creation, and assist in establishing its relevance to the case.

4.3.15 Timestamps

Timestamps are a specific type of metadata that records the time and date of an event, such as file creation, modification, or access. Timestamps can be essential for establishing the chronology of events related to digital evidence. They can indicate when a file was created, modified, or accessed, providing valuable information for determining the timeline of events in an investigation. For example, if a suspect's computer contains a file that was accessed shortly before the alleged crime, the timestamp associated with that access could be significant evidence. It could corroborate the suspect's presence or involvement in the event, strengthening the case against them.

These mechanisms collectively form a robust framework, with forensic imaging and hashing providing technical assurance, while chain of custody and documentation offer procedural safeguards. Metadata and timestamps add contextual depth, enabling thorough verification.[176]

4.3.16 Challenges Affecting Credibility

Beyond the procedural and technical factors already discussed, digital evidence faces several fundamental challenges that can affect how courts evaluate it. These challenges arise from the very nature of digital information and the technological environment in which it exists.

[176] Institute of Forensics Auditors (IFA), Authentication of Digital Evidence (14 Oct 2024). Available at www.ifaglobal.institute accessed 22 November 2025.

First, digital data is remarkably easy to alter or fabricate.[177] Unlike physical documents that show visible signs of tampering, digital files can be seamlessly edited using widely available software. Text can be changed, images manipulated, entire files created to appear as if they were made weeks or months earlier. This malleability means courts cannot rely on visual inspection to detect forgery and must instead depend on technical analysis.

Second, technology evolves rapidly. New devices, file formats, and communication platforms appear constantly. Forensic methods that work today may become outdated as technology changes. Courts evaluating whether forensic techniques are reliable must recognize that digital forensics is a constantly evolving field rather than a static body of knowledge.

Third, digital evidence often implicates privacy rights. Searches of computers or phones can expose vast amounts of personal information extending far beyond what is relevant to the alleged crime.[178] Courts must balance investigative needs against constitutional privacy protections, potentially limiting what evidence can be collected or presented.

Fourth, the hearsay rule creates complications for digital evidence. Many electronic records contain out-of-court statements: emails, text messages, social media posts.[179] Whether such evidence constitutes inadmissible hearsay depends on complex analysis of how the evidence was created and for what purpose it is being offered. Some courts have struggled to apply traditional hearsay doctrines to modern electronic communications.

4.3.17 Role of Expert Evidence

[177] *Ibid*, note 2, 18.
[178] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.
[179] *Ibid*, note 3, s 38.

Given the technical complexity of digital evidence, expert testimony often becomes necessary to help courts understand it. Digital forensic experts can explain how devices operate, how data is stored and recovered, whether evidence shows signs of alteration, and whether proper forensic methods were employed.

For expert testimony to be admissible, the proposed expert must first be qualified.[180] This involves demonstrating relevant education, training, experience, and professional credentials. A witness claiming expertise in digital forensics might present evidence of computer science degrees, professional certifications, specialized training courses, and experience conducting forensic examinations.

The expert's methodology must also be reliable. Courts will examine whether the expert used validated techniques, followed established protocols, and employed appropriate tools. For digital forensics, this might include questions about whether write-blocking was used, whether hash verification was performed, whether the analytical approach is accepted within the forensic community.

Expert testimony should help the court understand technical evidence without overwhelming judges or jurors with jargon. Effective experts translate complex concepts into plain language, use visual aids to illustrate key points, and focus on what is relevant to the legal issues rather than unnecessary technical details.

Cross-examination tests the expert's qualifications, methodology, and conclusions. Defense counsel may challenge whether the expert truly possesses relevant expertise, whether appropriate methods were used, whether the analysis was thorough, and whether the conclusions are fully

[180] *Ibid*, s 68.

supported.[181] Strong cross-examination can reveal weaknesses in expert analysis or expose alternative explanations that create reasonable doubt.

4.3.18 Digital Evidence in Nigerian Courts

Nigerian courts have shown increasing openness to digital evidence, recognizing its importance in modern litigation. The Evidence Act 2011 explicitly addresses electronic evidence in Section 84, providing statutory foundation for its admissibility. However, practical application has revealed both progress and ongoing challenges.

Courts have admitted digital evidence when properly authenticated - when there is sufficient foundation showing how it was created, maintained, and retrieved. Financial records, email communications, and computer-generated documents appear regularly in Nigerian cases involving fraud, corruption, and cybercrime.[182]

But challenges remain. Authentication sometimes receives insufficient attention, with electronic evidence being admitted based on superficial foundation that does not adequately establish its genuineness. Chain of custody documentation is sometimes inadequate, failing to track digital evidence with the detail its volatile nature requires. Expert testimony is inconsistently employed, with some cases proceeding without adequate technical testimony that would help courts properly evaluate complex evidence.

These challenges suggest the need for continued judicial education on digital evidence issues. As judges, prosecutors, and defense counsel develop greater familiarity with electronic evidence and

[181] *Ibid*, note 14
[182] *Federal Republic of Nigeria v Oritsejafor* [2016] unreported, Charge No FHC/L/236C/2014.

its unique characteristics, we should see more rigorous and consistent application of authentication requirements, chain of custody standards, and expert testimony.

The comparative experience shows that Nigerian courts generally recognize the value of digital evidence and are willing to admit it when proper foundations are established. What remains is to develop more consistent practices for authenticating such evidence and ensuring it meets the reliability standards that the Evidence Act requires.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter brings this long essay to a conclusive end, summarizing each chapters of this long essay. Each chapter has it unique and distinct area of focus, which will enable any reader to understand its contents and help in knowledge advancement on digital evidence in the Nigeria Legal System with ease. It's to be acknowledged that, this long essay not only dwells on the Nigerian Legal System but also different countries in the world.

The long essay broadens the view of the primary use and advanced usage of electronic evidence in a court proceeding, giving an understanding as to what is acceptable as an evidence digitally, it's admissibility and credibility.

Digital evidence as an arising form of evidence which is now an admissible evidence, section 84 of the Evidence Act 2011(as amended 2023) provides the rules and regulations that awards digital evidence its admissibility, credibility and reliability in any trial.

It has been legally accepted into the Nigerian Legal System, with recognized statutes and its efficacy has proven to be very helpful to the courts in Nigeria.

5.2 Summary of Key findings

Each chapter holds a unique and distinct context, elaborately illuminating the different sides of digital evidence, delving into its history, its challenges and its efficacy. Chapter one provided a contextual background to the study, emphasizing the significance of digital evidence in Nigerian Legal System. It introduces the study's objectives, highlighting the efficacy of using digital

[183] Evidence Act ,2011(as amended 2023)

evidence in a court proceedings, and the adaptation of Nigerian court to the use of digital evidence. The chapter also outlined the research methodology and scope of study, outlining a systematic approach to understanding the subject of digital evidence. Chapter two delved into the literature review and theoretical framework, the historical development of digital evidence, various types of digital evidence, a precise legal framework governing digital evidence, the theoretical framework throwing more light into understanding the context of the subject. Chapter three focused on the importance of admissibility of digital evidence, the legal standards of admissibility of digital evidence and analyzed critical areas of technical requirements, challenges in the admissibility of digital evidence, the chapter also prepares plethora of cases that enables any reader make further research and a concrete knowledge of digital evidence. Chapter four throws more light on the credibility and reliability of digital evidence, authentication mechanisms in the verification of digital evidence. It also analyzed challenges affecting the credibility of digital evidence, the uniqueness of expertise assistance in the verification of digital evidence and technical assessment.

One main hurdle of this long essay, is the lack of available data to support the essay, the Nigeria legal system have not fully adapted to the usage of digital evidence in a court proceeding, which therefore limits the possibilities of digital evidence in court.

The overuse of the Evidence Act 2011(amended 2023), as it is the only existing statute in Nigeria that provides for the admissibility of digital evidence.

5.3 Legal and Policy Implications

Digital evidence has room for improvement in Nigeria Legal System. With the provided rules and regulations of section 84 of Evidence Act 2011(as amended 2023) established for the purpose of digital evidence, which has proven that digital evidence is a recognized form of evidence in the Nigerian court implying its legal and policy status. The challenges faced by the Nigerian Legal System implementation of the use of digital evidence in a court proceeding can be dealt with overtime as it updates it knowledge on the dynamics of technology.

5.4 Recommendations

To address the challenges identified, Nigeria should prioritize the domestication of digital evidence, that is, normalizing the use of digital evidence in any court proceeding and adapt into the constant usage of electronics, such as CCTVs, audio and visual records, this would aid in easy access to having reliable sources of evidence. Law enforcement agencies must prioritize digital evidence handling best practices, including, proper training, adherence to forensics procedures and strict security measures mitigate risks such as tampering or altering of evidence and cyber threats. Nigeria should also do well in the employment of experts in technical fields on areas where there may be difficulties in verifying the credibility of digital evidence.

5.5 Areas of Future Research

Further research should focus on dynamics of technology in aiding the legal world, a profound research on new system softwares that would ease the integration of digital evidence into the Nigerian Legal System.

184 *Ibid*

185 Introducing the future of Digital Forensics and Evidence Management (infographic)

Researches should be made on areas that hinders digital evidence and recommendations on permanent solutions to hindrances.

Researches should be carried out on data visualization, multi-device evidence and timeline resolution, data duplication for storage and acquisition purposes.

5.6 Final Conclusion

In conclusion, this study has delved into the challenges faced by the Nigerian Legal System in the admissibility and credibility of digital evidence in a court proceeding.

It further gives solutions to some of these hurdles, and illuminates the significance of digital evidence.

The modernity of the usage of digital evidence limits further research but heightens the unfolding of digital evidence as it aides the Legal System in Nigeria.

By addressing systematic issues affecting the admissibility and credibility of digital evidence, challenges faced by the Nigerian court would lessen and integration of digital evidence in a court proceeding would be more effective.

BIBLIOGRAPHY

Books

Aguda, T.A. (1999). *The Law of Evidence in Nigeria*. Spectrum Books.

Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed. Academic Press).

Garrie, D.B. and Gelb, M. (2007). *E-Discovery & Digital Evidence*. (Thomson West)

Mason S, *Electronic Evidence* (4th edn, LexisNexis 2017).

Mohay, G. et al. (2003). *Computer and Intrusion Forensics*. Artech House, pp. 89-95.

Park, R.C., Leonard, D.P. and Goldberg, S.H. (2004). *Evidence Law: A Student's Guide to the Law of Evidence as Applied in American Trials* (2nd ed.). West Publishing,

Rhode, D.L. (2004). *Access to Justice*. Oxford University Press

Articles in Journals

Al-Zarouni M, 'Mobile Handset Forensics: An Overview' (2006) 3(2) *International Journal of Digital Evidence*.

Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence* (Version 5, 2012).

Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn, Academic Press 2011).

Gercke, M. (2012). *Understanding Cybercrime*. International Telecommunication Union

Hans, V.P. and Reyna, V.F. (2011). 'To Dollars from Sense: Qualitative to Quantitative Translation in Jury Damage Awards', *Journal of Empirical Legal Studies*, 8(S1)

International Organization on Computer Evidence (2000). *Guidelines for Best Practice in the Forensic Examination of Digital Technology*.

Kerr, O.S. (2004). 'The Fourth Amendment and New Technologies', *Michigan Law Review*, 102(5)

Lederer, F.I. (2005). 'The Road to the Virtual Courtroom', *South Carolina Law Review*.

Malik Hamad Al-Mashagbeh and others, 'Investigators of Digital Evidence: Main Challenges and Solutions' *International Journal of Information Security*, 2024

Mnookin, J.L. (2001). 'Scripting Expertise: The History of Handwriting Identification Evidence and the Judicial Construction of Reliability', *Virginia Law Review*, 87(8).

National Institute of Standards and Technology (NIST), *Guidelines on Mobile Device Forensics* (2014) SP 800-101 Rev 1, 23.

NIST (2006). *Guide to Integrating Forensic Techniques*, pp. 3-5 to 3-8.

Obamanu G, 'Legal Issues and Challenges in the Admissibility of Digital Forensic Evidence in Courts in Nigeria' (2023) 8(01) *AJIEEL* 96

Orebaugh, A. and Allnutt, J. (2010). 'Classification of Instant Messaging Communications for Forensics Analysis', *International Journal of Forensic Computer Science*, 1(1)

Park, R.C. (2007). 'The Hearsay Rule and the Stability of Verdicts: A Response to Professor Nesson', *Minnesota Law Review*, 70(4).

Risinger, D.M. (2000). 'Navigating Expert Reliability: Are Criminal Standards of Certainty Being Left on the Dock?', *Albany Law Review*, 64(1)

Sammons J, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* (2nd edn, Syngress 2014).

Scheindlin, S.A. and Rabkin, J. (2004). 'Electronic Discovery in Federal Civil Litigation', *New York University Journal of Law and Liberty*, 4..

Scientific Working Group on Digital Evidence (SWGDE), *Best Practices for Computer Forensics* (Version 3.1, 2014).

Shearing, V. and Macaulay, R. (2020). 'Text Messages as Evidence', *Journal of Digital Forensics, Security and Law*, 15(2)..

Shearing, V. and Macaulay, R. (2020). 'Text Messages as Evidence', *Journal of Digital Forensics, Security and Law*, 15(2).

Wigmore, J.H. (1940). *A Treatise on the Anglo-American System of Evidence in Trials at Common Law* (3rd ed.), Vol. 7. Little, Brown and Company, §2129

Online Sources

Casey E, (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press, p. 7. Available at: https://www.sciencedirect.com/book/9780123742681/digital-evidence-and-computer-crime (Accessed: 8 November 2025).

Casey, E. and Turnbull, B. (2018). 'Digital Evidence on Mobile Devices', in Casey, E. (ed.) *Handbook of Digital Forensics and Investigation*. Academic Press, pp. 165-196. Available at: https://www.elsevier.com/ (Accessed: 8 November 2025).

Chaikin, D. and Koenig, E. (2010). 'Admissibility of Electronic Business Records', *University of New South Wales Law Journal*, 33(1), pp. 30-56, at p. 35. Available at: http://www.unswlawjournal.unsw.edu.au/ (Accessed: 8 November 2025).

Chesney, R. and Citron, D.K. (2019). 'Deep Fakes', *California Law Review*, 107(6), pp. 1753-1820. Available at: https://www.californialawreview.org/ (Accessed: 9 November 2025)

Chesney, R. and Citron, D.K. (2019). 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', *California Law Review*, 107(6), pp. 1753-1820. Available at: https://www.californialawreview.org/ (Accessed: 8 November 2025).

Civil Evidence Act 1995 (UK), c. 38. Available at: https://www.legislation.gov.uk/ukpga/1995/38/contents (Accessed: 9 November 2025).

Civil Evidence Act 1995 (UK), c. 38. Available at: https://www.legislation.gov.uk/ukpga/1995/38/contents (Accessed: 8 November 2025).

Constitution of the Federal Republic of Nigeria 1999 (as amended), s. 37. Available at: https://www.wipo.int/edocs/lexdocs/laws/en/ng/ng014en.pdf (Accessed: 9 November 2025).

Corbin, A.L. (1944). 'The Interpretation of Words and the Parol Evidence Rule', *Cornell Law Quarterly*, 50(2), pp. 161-190. Available at: https://scholarship.law.cornell.edu/clr/ (Accessed: 8 November 2025).

Council of Europe Convention on Cybercrime (Budapest Convention), 23 November 2001, ETS No. 185, Arts. 14-21. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 8 November 2025).

Council of Europe Convention on Cybercrime, 23 November 2001, ETS No. 185, Arts. 23-35. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 9 November 2025).

Criminal Justice Act 2003 (UK), c. 44, s. 129. Available at: https://www.legislation.gov.uk/ukpga/2003/44/section/129 (Accessed: 8 November 2025).

Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Nigeria). Available at: https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf (Accessed: 8 November 2025)

DOA Law Firm. (2023, August 30). A Review of the Evidence Act (Amendment) Act, 2023. Available at: https://www.doa-law.com/evidence-act/ accessed 12 September 2025.

Evidence Act 2011 (Nigeria), ss. 83-84, 93-94. Available at: https://lawnigeria.com/LawsoftheFederation/EVIDENCE-ACT,-2011.html (Accessed: 9 November 2025).

Farid, H. (2009). 'Image Forgery Detection', *IEEE Signal Processing Magazine*, 26(2), pp. 16-25. Available at: https://ieeexplore.ieee.org/document/4786596 (Accessed: 8 November 2025)

Federal Rules of Civil Procedure (US), Rule 34(a)(1)(A) (2006 amendments). Available at: https://www.law.cornell.edu/rules/frcp (Accessed: 8 November 2025).

Federal Rules of Evidence (US), Rule 401. Available at: https://www.law.cornell.edu/rules/fre/rule_401 (Accessed: 9 November 2025).

Federal Rules of Evidence (US), Rules 401-403, 801, 901. Available at: https://www.law.cornell.edu/rules/fre (Accessed: 8 November 2025).

Foundation Chambers. (2023, August 25). Revolutionizing Evidence Gathering: An overview of the Evidence (Amendment) Act 2023. Available at: https://foundationchambers.com/revolutionizing-evidence-gathering-an-overview-of-the-evidence-amendment-act-2023-emmanuel-ikwuakolam/ accessed 12 September 2025.

Garrie, D.B. and Gelb, M. (2007). 'E-Discovery & Digital Evidence: Cases and Materials'. Thomson West. Available at: https://legal.thomsonreuters.com/ (Accessed: 8 November 2025)

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. International Telecommunication Union, Available at: https://www.itu.int/en/Pages/default.aspx (Accessed: 8 November 2025).

Goodman, M.D. (2003). 'Making Computer Stored Records Admissible', *Information Systems Security*, 12(1), pp. 8-14. Available at: https://www.tandfonline.com/toc/uiss20/current (Accessed: 8 November 2025).

Houben, R. and Snyers, A. (2020). 'Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion', *European Parliament Study*. Available at :https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf (Accessed: 8 November 2025)

Imwinkelried, E.J. (2005). 'Authenticating Digital Evidence', *Criminal Justice*, 20(2), pp. 2-10. Available at: https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/ (Accessed: 8 November 2025).

Institute of Forensics Auditors (IFA), Authentication of Digital Evidence (14 Oct 2024). Available at www.ifaglobal.institute accessed 22 November 2025.

ISO/IEC 27037:2012, *Information technology , Security techniques , Guidelines for identification, collection, acquisition and preservation of digital evidence*. Available at: https://www.iso.org/standard/44381.html (Accessed: 8 November 2025).

Kerr, O.S. (2004). 'The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution', *Michigan Law Review*, 102(5), pp. 801-888. Available at: https://repository.law.umich.edu/mlr/ (Accessed: 8 November 2025).

Kerr, O.S. (2005). 'Digital Evidence and the New Criminal Procedure', *Columbia Law Review*, 105(1), pp. 279-318, at p. 285. Available at: https://columbialawreview.org/content/digital-evidence-and-the-new-criminal-procedure/ (Accessed: 8 November 2025).

Lempert, R.O., Gross, S.R. and Liebman, J.S. (2000). *A Modern Approach to Evidence* (3rd ed.). West Publishing, pp. 1226-1235. Available at: https://legal.thomsonreuters.com/ (Accessed: 8 November 2025).

Mason S. (ed.) (2017). *Electronic Evidence* (4th ed.). LexisNexis, pp. 15-18. Available at: https://www.lexisnexis.co.uk/products/electronic-evidence.html (Accessed: 8 November 2025)

Mason, S. and Seng, D. (eds.) (2017). *Electronic Evidence* (4th ed.). Institute of Advanced Legal Studies, pp. 67-89. Available at: https://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence (Accessed: 8 November 2025).

Mohay, G. et al. (2003). *Computer and Intrusion Forensics*. Artech House, pp. 89-95. Available at: https://us.artechhouse.com/ (Accessed: 8 November 2025).

National Institute of Standards and Technology (2006). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86, p. 2-3. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (Accessed: 9 November 2025)

Regulation (EU) 2016/679 (General Data Protection Regulation), Arts. 5-6. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (Accessed: 8 November 2025)

Scientific Working Group on Digital Evidence (2016). *SWGDE Best Practices for Computer Forensics*. Available at: https://drive.google.com/file/d/1M_OWBlF5fikNH2BREaoBoHKlRF0L0N5i/view (Accessed: 9 November 2025).

Solove, D.J. (2007). '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy', *San Diego Law Review*, 44(4), pp. 745-772. Available at: https://digital.sandiego.edu/sdlr/ (Accessed: 8 November 2025).

Sommer, P. (2008). 'Directors' responsibilities and authentication of digital evidence', *Digital Investigation*, 5(1-2), pp. 43-49. Available at: https://www.sciencedirect.com/science/article/pii/S174228760800013X (Accessed: 8 November 2025)

Stren & Blan Partners. Evidence (Amendment) Act 2023 – Aligning Evidence Taking in Judicial Proceedings with Technological Advancements. Available at: https://strenandblan.com/evidence-amendment-act-2023-aligning-evidence-taking-in-judicial-proceedings-with-technological-advancements/ accessed 12 September 2025.

Twining, W. (1990). *Rethinking Evidence: Exploratory Essays*. Northwestern University Press, pp. 71-95. Available at: https://nupress.northwestern.edu/ (Accessed: 8 November 2025)

Tyler, T.R. (2003). 'Procedural Justice, Legitimacy, and the Effective Rule of Law', *Crime and Justice*, 30, pp. 283-357. Available at: https://www.journals.uchicago.edu/toc/cj/current (Accessed: 8 November 2025).

Youth Justice and Criminal Evidence Act 1999 (UK), c. 23, s. 60, Sch. 3. Available at: https://www.legislation.gov.uk/ukpga/1999/23/contents (Accessed: 9 November 2025).