EMERGING MINDS
JOURNAL FOR STUDENT RESEARCH

ISSN 2976-9094
EMJSR 2026,Vol 4:SO1-SO42
https://doi.org/10.59973/emjsr.289

Received: 2025-10-23
Accepted: 2026-01-21
Published: 2026-01-25

Limitations of Digital Forensic Investigation in Nigeria's Rural Comunities

Chidiebere Johnson Odo [1,*]

[1] University of Portsmouth, Faculty of Humanities and Social Sciences, School of Criminology and Criminal Justice, Portsmouth PO1 2HD, United Kingdom

*Corresponding author: Chidiebere.Odo1@myport.ac.uk

Abstract - Digital forensic investigation has become an indispensable tool for contemporary criminal justice systems. In Nigeria, however, rural communities remain significantly disadvantaged in the application of digital forensics due to deep-seated infrastructural, institutional, and socio-cultural limitations. This study employs a literature-based methodology, drawing on peer-reviewed scholarships, government reports, and comparative studies from other developing countries, to critically examine these challenges. The findings indicate that inadequate infrastructure such as unreliable electricity, poor telecommunication networks, limited internet penetration, and weak transportation systems constitutes the primary barrier to effective forensic practice in rural areas. Equally significant are the shortages of skilled personnel and inadequate training opportunities among law enforcement, which frequently lead to the mishandling of digital evidence and diminished prosecutorial outcomes. Institutional fragmentation, lack of rural-specific frameworks, and funding disparities further constrain forensic capacity. Socio-cultural factors, including low digital literacy, mistrust in technological processes, and judicial underappreciation of digital evidence, exacerbate the problem. Comparative lessons from Kenya, India, Brazil and South Africa demonstrate that policy interventions, rural-based training programs, and innovative mobile forensic laboratories can mitigate these obstacles. For Nigeria, these insights highlight the need to decentralize forensic institutions, strengthen infrastructure, and adopt policies tailored to rural realities. The study concludes that unless targeted reforms are enacted, digital forensics in Nigeria will remain urban-centric, leaving rural communities vulnerable to cybercrime and digital exploitation. By situating Nigeria's challenges within global debates on digital justice, the paper underscores the urgency of inclusive reforms to bridge the rural-urban divide in forensic investigation.

Keywords - Digital forensics; Rural communities; Nigeria; Infrastructure; Law enforcement; Digital evidence.

1 Introduction

Digital forensic investigation has become a critical component of modern law enforcement, enabling the identification, preservation, and analysis of electronic evidence in the investigation of cybercrimes. In Nigeria, the growth of internet penetration, mobile technology adoption, and digital financial services has expanded opportunities for both legitimate digital engagement and cybercrime activities including fraud, cyberstalking, kidnapping, terrorism and online scams. Consequently, the role of digital forensics in ensuring justice, security,

and regulatory compliance has grown significantly. However, despite the increasing importance of digital forensic practices though largely centralized in urban areas like Abuja, Lagos and Porthourt, significant limitations persist in Nigeria, particularly within rural communities including Amede, Umuleshia, Sabon-Gari, Olorinda etc [1-3]. These challenges stem from multiple interrelated factors, such as inadequate technological infrastructure, insufficient skilled/motivated personnel, limited financial resources, and weak institutional frameworks. Rural communities often face poor network connectivity, irregular electricity supply, and logistical challenges that impede the deployment and operation of digital forensic tools. Additionally, law enforcement officers in rural areas may lack specialized training, resulting in the underutilization of available technologies and poor evidence handling practices [4]. Beyond technical and infrastructural challenges, socio-cultural factors also hinder the effectiveness of digital forensic investigations as the rural populations mostly rely on informal justice mechanisms and traditional conflict resolution systems, reducing the incentive to report cybercrimes to formal authorities and consequently limiting the detection and collection of digital evidence [5]. Furthermore, low levels of digital literacy and public awareness contribute to difficulties in preserving and presenting electronic evidence in ways that meet legal standards. Therefore, understanding these limitations is essential for developing strategies to strengthen digital forensic capabilities across Nigeria particularly the villages. By examining the interplay of technological, institutional, and socio-cultural constraints, this study seeks to provide a comprehensive analysis of the challenges facing digital forensic investigation in Nigeria's rural communities, highlighting potential pathways for reform and capacity building as the research draws on summary case studies, theoretical frameworks, and empirical findings to demonstrate the infrastructural and systemic deficits that impede the areas.

1.1 Rationale/Justification

The rationale for investigating the limitations of digital forensic investigation in Nigeria's rural communities lies in the widening gap between technological advancement and rural justice delivery. Digital forensics has become indispensable in modern criminal justice systems, aiding in the investigation of cybercrime, terrorism, kidnapping, financial fraud, and other digitally facilitated offenses [6]. However, while urban centers in Nigeria such as Abuja, Lagos, and Port Harcourt have gradually embraced digital forensic practices, rural communities remain underserved due to infrastructural deficits, weak institutional frameworks, and socio-cultural barriers [7]. This uneven development undermines the principle of equitable access to justice and exposes rural populations to higher vulnerability in digital crime investigations.

The justification of this research is further strengthened by Nigeria's increasing rural-urban digital divide. Despite government investments in ICT and security modernization, inadequate road networks, unreliable electricity supply, low digital literacy, and fragmented law enforcement efforts continue to hinder the deployment of forensic technologies in rural areas [8]. Therefore, without addressing these structural deficiencies, rural communities' risk being excluded from national cybersecurity strategies, leading to investigative lapses, wrongful convictions, or failure to detect and prosecute offenders. Moreover, the study is justified by the pressing need to draw lessons from other developing countries that have successfully integrated rural realities into digital forensic frameworks. By identifying limitations in Nigeria's context, the research contributes to policy formulation, capacity building, and infrastructural planning tailored to rural security needs. In doing so, it aligns with global calls for inclusive security governance that recognizes rural spaces as critical nodes in the digital crime ecosystem [9]. Thus, this study is not only timely but also essential for bridging justice gaps, enhancing forensic effectiveness, and safeguarding national security.

1.2 Research Aim

The primary aim of this research is to critically examine the limitations of digital forensic investigation in Nigeria's rural communities, with a particular focus on how infrastructural, institutional, and socio-cultural constraints hinder the effective deployment and practice of forensic technologies. The study seeks to identify the underlying structural deficiencies such as inadequate road network, electricity supply, poor internet connectivity, limited technical expertise, and the absence of standardized frameworks that restrict digital forensic operations in rural areas compared to urban centers. Additionally, the research aims to explore the roles of resource allocation disparities, law enforcement challenges, and policy neglect in exacerbating the digital divide between rural and urban communities.

By systematically analyzing these limitations, the research intends to provide a comprehensive understanding of why rural communities remain marginalized in Nigeria's digital forensic landscape. Furthermore, it seeks to evaluate comparative practices in other developing countries to draw lessons that can inform Nigeria's policy and strategic interventions. Ultimately, the study aims to recommend context-driven solutions that will strengthen forensic capacity, enhance rural law enforcement effectiveness, and promote equitable access to digital investigative tools across all regions of Nigeria.

1.3 Research Objectives

1. To identify the infrastructural challenges, such as electricity, internet connectivity, and transport networks, that limit digital forensic investigation in rural Nigeria.
2. To examine the role of institutional weaknesses, including inter-agency fragmentation, lack of standardized frameworks, and funding disparities, in hindering rural forensic practices.
3. To assess the impact of socio-cultural realities, such as low digital literacy, mistrust of law enforcement, and reliance on informal justice systems, on the preservation and use of digital evidence in rural communities.
4. To evaluate how policy neglect and urban-centered strategies have contributed to the marginalization of rural areas in Nigeria's digital forensic development.
5. To compare Nigeria's rural forensic limitations with those of other developing countries and identify best practices that can be adapted for Nigeria.
6. To recommend practical, context-sensitive strategies and policy reforms that can strengthen digital forensic capacity and enhance equitable access to investigative tools in Nigeria's rural communities.

1.4 Theoretical or Conceptual Framework

The present study is anchored on the Technology Acceptance Model (TAM) and Institutional Theory, which together provide a dual perspective for examining the limitations of digital forensic investigation in Nigeria's rural communities. These theories are useful in unpacking both the micro-level challenges of technology adoption among practitioners and the macro-level institutional deficiencies that shape forensic practice in Nigeria.

The Technology Acceptance Model (TAM), introduced by Davis [10], posits that an individual's intention to adopt a technology is determined by two key perceptions: perceived usefulness (PU) and perceived ease of use (PEOU). In the context of digital forensics, PU reflects whether rural law enforcement and judicial officers believe forensic technologies can

significantly improve investigative outcomes, while PEOU denotes the extent to which these tools are seen as simple, accessible, and adaptable to local conditions [11]. In rural Nigeria, however, inadequate infrastructure, unreliable electricity, poor road networks, and limited access to digital training reduce both PU and PEOU. Consequently, even when forensic technologies are made available, they may not be fully embraced or deployed effectively because they are perceived as difficult to operate or irrelevant to pressing security needs. Thus, TAM helps to explain the low uptake of forensic tools by practitioners operating in rural contexts marked by infrastructural and literacy deficits.

On the other hand, Institutional Theory, as advanced by Meyer and Rowan [12] and further developed by DiMaggio and Powell [13], emphasizes that organizational practices are not only driven by efficiency but also by institutional norms, rules, and legitimacy. In Nigeria, forensic capacity development is hampered by fragmented inter-agency collaboration, weak regulatory frameworks, and inconsistent funding mechanisms [14]. The absence of a unified national forensic strategy creates institutional ambiguity, where security agencies, courts, and rural policing structures lack standardized procedures for evidence handling and digital investigation. Institutional Theory explains how these systemic weaknesses limit the effective embedding of forensic practices in rural environments, as organizations often conform to symbolic compliance with policy directives rather than implementing functional forensic practices.

Integrating TAM and Institutional Theory provides a holistic conceptual framework for this study. While TAM accounts for the individual-level barriers to technology adoption, Institutional Theory situates these challenges within the broader context of structural and organizational constraints. For example, even if rural police officers are willing to adopt forensic technologies, institutional deficiencies such as lack of funding, weak judicial backing, and absence of training/motivational frameworks will continue to hinder effective practice. This synergy highlights that the limitations of digital forensic investigation in Nigeria's rural communities cannot be understood solely as a technological issue but as a complex socio-technical and institutional challenge. Accordingly, this framework underscores that sustainable digital forensic practice in rural Nigeria requires not only capacity building for technology acceptance but also institutional reforms that strengthen legitimacy, coordination, and resource allocation. By applying both TAM and Institutional Theory, the study situates rural forensic limitations within the interplay of human, technological, and institutional dynamics, thereby offering a more comprehensive lens for analysis.

1.5 Methodology/ Research Design

This study adopted a literature-based studies research design to identify the limitations of digital forensic investigation in rural communities of Nigeria. A literature-based approach was deemed appropriate due to the security and safety nature of the research, which aims to understand deep-rooted infrastructural, institutional, and socio-cultural challenges (Creswell & Poth, 2018). Through book reviews, policy analysis, and case studies, the research seeks to gather rich, contextual data from relevant stakeholders in both urban and rural forensic ecosystems.

1.6 Structure of the Dissertation

The structure of this paper is six (6) multi-sections and chapters format that reflects the research process, with a standard model used in the social sciences. This includes introductory material, core chapters, thematically arranged for review and analysis, and supplementary sections. However, the introductory chapter provides background information regarding the research rationale or justification, aim, objectives, theoretical or conceptual framework, methodology/design and structure of the dissertation. Chapter two highlights relevant lit-

erature, to situate the forthcoming research within the extant theoretical paradigms and emphasize areas where further scholarship is needed. Chapter three thematically organizes around three key dimensions and three sub-categorized units corresponding to the study's first set of lower-level objectives. Chapter four presents comparative perspectives and case studies of other developing countries. Chapter five addresses the issues of deployment by unpacking three interrelated themes and Chapter six discusses research findings, followed by the limitations, conclusion and recommendations for future research.

1.7 Summary

This chapter introduces the study by outlining the significance of digital forensic investigation in modern criminal justice systems and the particular vulnerabilities of Nigeria's rural communities. It highlights the research problem namely, that despite growing cybercrime and security threats, rural Nigeria remains critically underserved in terms of digital forensic capacity due to infrastructural, institutional, and human resource limitations. The research aim and objectives are clearly articulated, alongside the scope, rationale, and contribution of the study. To situate this problem within a wider body of knowledge, the chapter concludes by noting the need for a critical review of existing literature on digital forensics globally and locally, which forms the basis of the next chapter.

2 Current Practices of Digital Forensics in Nigeria: Literature Review

2.1 Introduction

It is important to understand why infrastructure challenges remain the most visible barrier to digital forensic investigation in most developing countries especially Nigeria's rural communities, but a deeper analysis reveals that these problems extend beyond technical deficiencies to reflect long-standing political, economic, and social exclusions. At the surface level, unreliable electricity supply, weak internet connectivity, and inadequate ICT facilities impede the deployment of forensic technologies in rural areas [15]. However, the persistence of these challenges raises a fundamental question: why has Nigeria, despite decades of ICT growth, failed to extend critical infrastructure to its rural regions? One explanation lies in Nigeria's pattern of urban-biased development. Infrastructural projects are often concentrated in cities such as Lagos and Abuja, where economic returns and political visibility are higher [16]. This selective investment strategy structurally disadvantages rural communities, turning them into "blind spots" for digital innovation, including forensic practice. Consequently, infrastructure is not merely absent but deliberately deprioritised. This urban-centric development logic demonstrates that the challenge is not technical incapacity but a reflection of national planning priorities. Even if infrastructural investment were made tomorrow, the effectiveness of rural forensic practice would still be questionable. For instance, improved internet and electricity access would not automatically address low digital literacy among rural law enforcement or the mistrust of technology among rural populations. Thus, infrastructural solutions alone risk being superficial unless integrated with human capital development and cultural adaptation strategies.

Comparative insights highlight the significance of this critique. India, facing similar rural-urban divides, has pursued nationwide rural internet projects such as BharatNet, which dramatically expanded forensic investigation reach into non-urban areas [17]. Nigeria, however, has failed to implement similar large-scale rural digital initiatives, suggesting that its infrastructural weakness is more a product of weak political will than insurmountable technical obstacles. Meanwhile, Brazil overcame geographic barriers by investing in satellite and drone-assisted forensic technologies, demonstrating that infrastructural limitations can be mitigated through innovation [18]. Yet Nigeria's persistent insecurity and governance gaps make such alternatives difficult to sustain. The consequence of infrastructural neglect

is not only technological exclusion but also a widening gap in justice delivery. Rural communities, already vulnerable to cyber-enabled fraud, terrorism financing, and mobile money crimes, are left without credible investigative mechanisms. This undermines public trust in the state's ability to deliver justice, further entrenching the perception of rural neglect. More critically, these blind spots create safe havens for criminals, with rural areas becoming operational bases for crimes that spill over into urban and even international domains. Therefore, infrastructure limitations in rural Nigeria must be reframed not as isolated technical shortcomings but as evidence of systemic marginalisation. Policy responses should extend beyond infrastructure provision to include deliberate rural integration into national ICT strategies, accountability mechanisms to ensure equitable distribution of resources, and innovative approaches that bypass traditional infrastructure barriers. Without such comprehensive measures, Nigeria risks perpetuating a forensic divide that undermines both rural security and national stability.

Furthermore, digital forensic practices in Nigeria are primarily driven by institutions such as the Economic and Financial Crimes Commission (EFCC) [19], the Nigeria Police Force (NPF) [20], and the Department of State Services (DSS) [21]. These institutions operate digital labs mostly located in Abuja, Lagos, and other urban centers. Despite legislative support like the Cybercrimes Act (2015) [22], challenges such as limited reach, lack of technical expertise in rural areas, and resource constraints hinder the effectiveness of forensic practices nationwide. However, digital forensics is the application of scientific methods to the identification, preservation, analysis, and presentation of digital evidence in a manner that is legally admissible in court, making it an indispensable tool in modern criminal justice systems (Casey, 2011). For example, in the United States, Drew (2009) stated that forensic investigators analyzed computer logs and internet activity to prove the defendant's involvement in cyber harassment, leading to a conviction based on digital evidence. Similarly, it also refers to the systematic process of identifying, acquiring, preserving, analyzing, and presenting digital evidence as illustrated in a cyber fraud investigation where forensic experts image a suspect's hard drive, recover deleted emails, and present the recovered evidence in court to establish the chain of events leading to the crime. The same as in Omondi Ogutu, et al., (2016) in Kenya, forensic investigators extracted call data records and mobile phone text messages, which were presented in court to establish the suspects' communication patterns before and after a robbery, leading to their conviction.

Consequently, the rise in cybercrime and other technology-facilitated offenses in Nigeria has necessitated the adoption of digital forensic techniques across law enforcement, intelligence, and judicial sectors [1]. He added that, while the practice of digital forensics is gaining traction in urban centres, rural communities where infrastructure, training, and awareness are often lacking remain largely excluded. This paper, therefore, explores how digital forensics is practiced in Nigeria and critically analyzes the extent to which its effectiveness is compromised in rural communities.

2.2 Digital Forensics Establishment in Nigeria: An Overview

Nigeria's digital forensics landscape has developed unevenly, shaped by rapid digitization, cyber-enabled crime, and a gradually maturing legal institutional framework. The cornerstone statutes are the Evidence Act 2011 (Section 84 on electronic evidence) [23] and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 which provides the basic legal basis for acquiring, preserving and admitting digital evidence in court [22-23]. However, policy direction has been articulated through the National Cybersecurity Policy and Strategy (NCPS) 2021 [24] under the Office of the National Security Adviser (ONSA), which assigns roles across law-enforcement, regulators, and critical infrastructure operators, and establishes national coordination through ngCERT (ONSA, 2021). But completely absence in

rural consideration which negatively impacts on the investigative outputs from the area.

Operationally, capability is concentrated in federal agencies these include the Economic and Financial Crimes Commission (EFCC) which runs digital forensic laboratories integrated with its detective and prosecutorial workflow, supporting examinations of computers, mobile devices and network artifacts in financial-crime and cyber-fraud cases [19] (EFCC, 2019). The Nigeria Police Force (NPF), particularly within the Force Criminal Investigation Department (CID), has built computer and mobile forensics capacity used in homicide, kidnapping, terrorism, cyberstalking, and advance-fee fraud investigations, often in collaboration with service providers and the Nigerian Communications Commission (NCC) for lawful interception metadata and call-detail records (NCC, 2020; NPF, 2021). Sectoral regulators such as the Central Bank of Nigeria (CBN) [25] for payment systems and NITDA/NDPB for data governance reinforce incident reporting and evidence preservation obligations that buttress forensic workflows in the financial and data-protection domains (CBN, 2022; NITDA, 2019; Nigeria Data Protection Act, 2023) [26].

While in practice, digital forensics in Nigeria spans first responder triage, imaging and analysis, malware reverse engineering in select cases, and expert testimony. Typical exemplars include EFCC's dismantling of organized online fraud networks through multi-device acquisition and cryptocurrency wallet analysis, and police investigations where handset artifacts (chat logs, geolocation traces, and media metadata) have been pivotal to securing convictions (EFCC, 2019; NPF, 2021). Similarly, the Department of State Services (DSS) sits at the core of Nigeria's internal security and counter-intelligence architecture and increasingly integrates digital forensics across its investigative workflow. In practice, DSS operatives support cyber-enabled crime and terrorism cases by triaging and seizing digital devices, preserving chain-of-custody, imaging media, and conducting lab-based analysis to generate actionable intelligence for prosecutions and threat disruption, under the national framework provided by the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 and subsequent amendments (which establish institutional coordination and investigatory powers) [27] (Cybercrimes Act, 2015/2024). At the strategic level, independent assessments note Nigeria's developing cyber-intelligence posture but highlight continuing coordination and skills gaps, underscoring why codified workflows and inter-agency readiness (including forensics) remain priorities for DSS operations (IISS, 2023). Public DSS communications emphasise incident reporting, vigilance, and collaboration with other services, aligning their digital forensic tasks with broader mandates of threat prevention, evidence generation, and protective security. Together, these elements situate DSS digital forensics as a structured, legally anchored workflow spanning collection to courtroom-ready outputs within Nigeria's evolving cybersecurity ecosystem [21]. Unfortunately, the chain-of-custody protocols, though formally recognized, remain vulnerable to fragmentation when multiple agencies touch the same evidence without harmonized standard operating procedures (SOPs) (ONSA, 2021).

Nevertheless, while Section 84 of the Evidence Act has eased admissibility barriers, judicial familiarity with hash values, metadata provenance, and volatile memory artifacts varies, necessitating sustained bench and bar training (Evidence Act, 2011). Inter-agency coordination is improving but still challenged by overlapping mandates, budget silos, and inconsistent SOPs across police, EFCC, DSS, and sectoral regulators (ONSA, 2021). However, recent reforms point to consolidation. This means that, the NCPS's whole-of-government model, coupled with CERT coordination, aims to standardize incident response and evidence handling as Data-protection regulation (NDPR, now codified in the 2023 Act) is pushing organizations to log, preserve, and document systems in ways that indirectly strengthen forensic readiness (NITDA, 2019; Nigeria Data Protection Act, 2023). Looking ahead, priorities include: (i) national SOPs and accreditation for digital forensic labs; (ii) a scalable training pipeline linked to universities and judicial institutes; (iii) sustainable funding for toolchains;

and (iv) outreach models that extend forensic services to underserved rural jurisdictions through mobile labs and regional hubs. Hence, with these elements, Nigeria can transition from ad-hoc excellence in marquee cases to a resilient, nationwide digital forensics regime.

2.3 Centralized Policy Implementation and Urban Bias

Although Agbo 2022 viewed the centralized practice as a typical follow of internationally recognized procedures, evidence acquisition, chain of custody maintenance, forensic analysis, and reporting as well as a legal framework such as the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, which supports the admissibility of digital evidence in Nigerian courts, provided it is collected and preserved according to due process, the urban bias largely concentrated the forensic hubs in major cities of Nigeria such as Abuja, Lagos, and Port Harcourt while most rural areas lack access to the essential infrastructure, personnel, and tools required to conduct even basic digital forensic investigations. No wonder the Guardian newspaper of 2016 supported that Nigeria has witnessed gradual but significant growth in its digital forensic ecosystem, with the emergence of private service providers, specialised training institutions, and government-linked laboratories. These establishments have been instrumental in building investigative capacity, enhancing evidence handling standards, and introducing advanced technological tools for crime detection and prosecution. But, the distribution of these facilities remains highly urban-centric, with limited or no presence in rural communities, thereby perpetuating the infrastructural gap in digital forensic access. However, the impact of this urban and rural divide has encouraged even the private service providers which constitute the backbone of Nigeria's operational digital forensic sector to establish their laboratories in the urban areas. For instance, First Digital & Techno-Law Forensics Co. Ltd., established in 2008 as the country's first indigenous digital forensic company, operates a full-service laboratory offering computer and mobile forensics, handwriting analysis, cybercrime investigation, and expert witness services as well as also played a notable role in drafting national digital forensic standards and training law enforcement and judicial personnel (First Digital & Techno-Law Forensics, n.d.) is situated in Abuja. Similarly, Forensic System Solutions (FSS), incorporated in 2013, delivers forensic document examination, digital evidence recovery, fingerprint analysis, and cyber incident response for clients in both public and private sectors (Forensic System Solutions, n.d.) is in Lagos. The more recent Comotech Digital Forensics Company Ltd. (established 2018) that offers combined digital investigation and IT solutions, including CCTV installation and network security, and A&D Forensics focuses on blockchain and cryptocurrency investigations, partnering with the Securities and Exchange Commission of Nigeria (SEC) and international crypto-tracing firms such as Chainalysis (A&D Forensics, n.d.). are all in urban part of Nigeria.

A way from digital forensic service delivery, urban Nigeria equally hosts several training and research institutions dedicated to building professional capacity in digital forensics. For example, the Digital Evidence & Cyber Forensic Institute (DECFI), approved by the Federal Government, is the country's first institute specialising in training legal practitioners, law enforcement officers, and investigators in eDiscovery, cybercrime investigation, and forensic certification, with international partnerships for specialised laboratory work (Digital Evidence & Cyber Forensic Institute, n.d.). Similarly, the Chartered Institute of Forensics and Certified Fraud Investigators of Nigeria (CIFCFIN), through its Board of Diplomates for Digital Forensics, regulates professional standards and certifies practitioners (CIFCFIN, 2022) is in urban part of Nigeria. While the Economic and Financial Crimes Commission (EFCC), which statutorily operates a forensic science laboratory and an academy that trains personnel in cybercrime investigation, financial forensics, and evidence handling is centered in Abuja. This includes the Lagos State DNA & Forensic Centre, launched in 2017 as West Africa's first state-owned DNA forensic laboratory, incorporates limited digital forensic functions

alongside its primary focus on biological evidence has its headquarters in Lagos Nigeria (Lagos State Government, 2017). This geographic centralisation means that evidence from rural areas, though rarely due to lack of digital forensic tools in the place, must be transported to urban laboratories, increasing the risk of tampering, loss, and chain-of-custody violations.

2.4 Absence of Rural-Specific Cybercrime Policy Instruments

Most cybercrime strategies in Nigeria operate under a "one-size-fits-all" framework, which does not account for regional disparities in digital access or literacy. The National Cybersecurity Policy and Strategy (NCPS) 2021 [24] outlines broad national goals such as increasing law enforcement capacity and promoting public awareness but offers no targeted interventions for rural areas. This oversight ignores critical realities of rural communities having different crime patterns, this includes, while urban digital crimes often involve financial fraud and identity theft, rural areas may face issues like sextortion, political misinformation, or phone-based fraud, host/ransom kidnapped victims, and terrorism targeting unbanked populations. It equally undermines limited access to digital rights awareness. For example, without explicit education or outreach programs, rural residents remain unaware of what constitutes a cybercrime or how to report it. In effect, national cyber strategies lack the granularity and localization necessary to be effective outside urban centres. As further noted, Nwokedi & Bello (2022), stated that the failure to develop "context-sensitive" forensic policies has left rural law enforcement structurally unequipped to respond to digital threats.

2.5 Funding and Resource Allocation Disparities

The chronic underfunding of digital forensic infrastructure in Nigeria reveals more than a financial shortfall; it reflects structural inequities in governance and national security priorities. While urban forensic labs in Lagos and Abuja receive relatively better funding, rural communities remain systematically excluded, creating a digital justice divide. This disparity is not merely a budgetary oversight but a symptom of centralised policymaking that privileges urban centres at the expense of rural realities [28]. Critically, improved funding alone may not resolve rural forensic deficiencies. Corruption, mismanagement, and weak accountability mechanisms mean that even when resources are allocated, they often fail to translate into functional infrastructure on the ground [8]. For example, federal budgets for law enforcement technology have historically been misdirected toward urban command headquarters, leaving rural divisions with outdated or non-existent forensic tools. Thus, the issue is less about scarcity of resources than about their distribution and utilisation. The insights from other developing nations highlight this complexity. In Kenya, decentralised budgetary frameworks allowed counties to co-fund local forensic initiatives, thereby reducing overreliance on central government allocations [29]. Nigeria's highly centralised fiscal structure, however, limits such rural empowerment. Similarly, in India, resource disparities were addressed through mobile digital forensic labs, but Nigeria's security threats on highways raise questions about the viability of such a solution in its rural regions. These comparisons underline the need for context-sensitive funding models rather than a simple call for increased expenditure.

Furthermore, underfunding creates cascading consequences. Rural law enforcement officers, already demoralised by poor remuneration, find themselves without the technological means to perform credible investigations, eroding public trust in justice delivery [30]. This has broader implications for national security, as cybercriminals exploit rural "blind spots" to stage operations that ripple into urban and even international arenas. In this way, funding disparities are not an isolated budgetary concern but a structural weakness with national and transnational implications. Therefore, addressing rural forensic funding gaps requires more than fiscal injections. It demands a reconfiguration of Nigeria's policy priorities, an accountability mechanism to track actual deployment of resources, and potentially a hybrid

funding framework that combines federal, state, and private-sector contributions. Without such systemic reform, additional allocations risk perpetuating the same cycle of exclusion and inefficiency.

Additionally, one of the most persistent barriers to the effective deployment of digital forensics in rural Nigeria is the disparity in funding and resource allocation between urban and rural law enforcement agencies. Urban centres such as Lagos and Abuja often receive disproportionate investment in forensic laboratories, ICT infrastructure, and personnel training, while rural regions are left underfunded, resulting in unequal investigative capacities [31]. This disparity stems from a centralised budgeting system that prioritises urban crime hotspots over dispersed rural communities, despite the increasing cyber and technology-facilitated crimes occurring in these areas [28]. Similarly, the lack of funding translates into inadequate equipment, such as mobile forensic kits, server analysis tools, and chain-of-custody management software, which are critical for evidence gathering in resource-constrained environments [32]. Furthermore, rural police units often struggle with poor remuneration, affecting morale and discouraging personnel from engaging in the highly technical work of digital forensics [33]. In some cases, investigations are delayed because rural officers must transfer devices to urban laboratories for examination, a process that risks evidence contamination, cost effective and undermines timely prosecution [34].

Comparative studies show that similar funding inequalities in other developing countries have weakened rural justice delivery, with local communities relying on informal conflict resolution mechanisms instead of formal forensic-supported prosecution [35]. For Nigeria, this funding imbalance not only widens the rural-urban digital justice gap but also weakens trust in state institutions. He added that the budgetary priorities in Nigeria overwhelmingly favour federal and state-level institutions based in urban areas. According to the 2023 Budget Office Report, less than 5% of digital security allocations were earmarked for community-based or rural policing enhancements. This leaves rural Divisional Police Headquarters without basic computer systems, secure data storage devices, internet access and personnel training budgets or packages. By contrast, agencies like the EFCC, DSS, and NITDA receive annual funding in huge sums of naira to support digital forensic upgrades, capacity development, and international partnerships (Budget Office of the Federation, 2023). This funding model creates a feedback loop where rural areas continue to underperform in digital investigations due to chronic underinvestment. Addressing this challenge requires decentralised budgeting, targeted rural forensic investments, and public-private partnerships to ensure that rural law enforcement units are adequately resourced to handle digital evidence.

2.6 Inter-Agency Fragmentation and Lack of Rural Outreach

The governance structure of digital forensic operations in Nigeria is marked by a lack of central coordination. Multiple agencies including the Nigeria Police Force (NPF), Economic and Financial Crimes Commission (EFCC), National Information Technology Development Agency (NITDA), and Nigerian Communications Commission (NCC) exercise overlapping mandates on cybercrime investigation and digital evidence handling [36]. Each of these institutions operates under different procedures, resulting in jurisdictional confusion, duplicative efforts, and weakened investigative outcomes. He added that this fragmentation is particularly harmful in rural areas, where the lack of institutional presence means that cases requiring digital forensic expertise are often abandoned due to uncertainty over who is responsible. For example, a cyber fraud case in a rural community may not receive prompt attention if the local police lack the jurisdictional clarity or inter-agency channels needed to escalate the matter to EFCC or NITDA. In the absence of streamlined governance, rural law enforcement agencies frequently default to inaction. Furthermore, there is no unified national forensic strategy that standardizes procedures, tools, or evidence handling proto-

cols across all security and regulatory agencies like the National Security Adviser (NSA). A similar situation of the UK Parliament's House of Lords Science and Technology Committee which concluded that forensic science oversight in England and Wales is piecemeal and fragmented, lacking consistent leadership, governance, and coordination across agencies. The committee highlighted the absence of a coherent national framework that integrates forensic services across different regions and providers such as police forces, private labs, and others. While a 2016 Forensic Science Strategy by the House of Commons proposed a "national approach," such efforts remain decentralised. The strategy depends largely on police forces themselves to implement consistency, standardisation, procurement, and accreditation as there's no central command or unified enforcement across all organisations. Further investigations by the House of Commons revealed that procurement remains largely in the hands of individual police forces, creating a fragmented forensic services market. As a result, small specialist providers struggle to compete, and there is no centralised protocol to unify evidence handling, tools, or procedures. Similarly, Chukwuma views the systemic gaps in closer studies of same situation that centralized coordination, and rural outreach can significantly improve forensic capacity. For example, Kenya's establishment of a National Computer and Cybercrimes Coordination Committee has enabled rural police units to access mobile forensic laboratories through inter-agency cooperation [35]. Nigeria's inability to replicate such models underscores how fragmentation and limited outreach remain critical barriers to rural digital forensic practice. He added that these lack of harmonizations results in evidentiary inconsistencies that affect the credibility of rural-based investigations in court.

2.7 Limited Public-Private Partnerships (PPPs) in Rural Forensics

While Nigeria has seen a rise in private forensic firms and technology incubators in urban centres, these entities rarely operate in rural regions. Firms such as DataPro, First Atlantic Semiconductors & Microelectronics (FASMICRO), and Digital Encode Limited offer expert services to banks, government agencies, and corporations but do not maintain offices or conduct outreach in rural communities. They insist that, "There is a missed opportunity here". PPP models could help to establish mobile forensic units, provide subsidized toolkits to rural law enforcement, support rural cybercrime education campaigns and train rural court clerks and prosecutors. But in the absence of state incentives or mandates, most private firms remain focused on profitable urban markets with the understanding that the rural Nigeria cannot afford their products and services [36]. He equally maintained the view that Nigeria's rural communities are disproportionately affected by policy gaps that compromise the effective practice of digital forensics. While urban centres benefit from forensic laboratories, technical partnerships, and institutional support, rural areas remain sidelined due to centralization, legal illiteracy, underfunding, and lack of targeted strategies and further stated that, bridging the urban-rural divide in digital forensic capability requires more than technology, hence, it demands structural reform, localized policy innovation, and inclusive budgeting with intentional decentralization and community-based forensic models. This will save the digital justice gap from continued to widen, leaving millions of rural Nigerians vulnerable in an increasingly digital world.

2.8 Weak Legislative Framework for Digital Evidence in Rural Jurisdictions

The absence of institutional frameworks for digital forensic practice in Nigeria's rural communities is often portrayed as a simple policy gap. However, a closer analysis suggests that this omission reflects deeper structural and political dynamics within Nigeria's governance system. Rather than being an oversight, the neglect of rural digital forensics is symptomatic of a state security agenda that prioritises urban protection and political visibility over comprehensive national coverage. At the descriptive level, Nigeria lacks a rural-specific digital forensic strategy; most existing frameworks such as the National Cybersecurity Policy (2014, revised 2021) focus predominantly on urban threats like financial fraud, cyberterrorism, and

critical infrastructure protection [34]. Yet, the persistence of this urban bias raises critical questions: why has rural cybercrime not been integrated into policy discourse, despite evidence that rural areas serve as operational bases for mobile fraud, terrorist financing, and internet scams? The answer lies partly in Nigeria's centralised governance model, where rural insecurity is often framed as a localised policing issue rather than a matter of national cybersecurity.

Institutional fragmentation further exacerbates this gap. Nigeria's law enforcement agencies, including the Police, Department of State Services (DSS), and the Economic and Financial Crimes Commission (EFCC), often operate with overlapping mandates and limited inter-agency coordination [37]. In rural contexts, this fragmentation results in duplicated efforts, absence of clarity in investigative authority, and, in many cases, complete neglect of digital evidence. Thus, the absence of frameworks is not simply a lack of documentation but a reflection of governance incoherence and inter-agency rivalry. The insights highlight the implications of this neglect. China's rural digital policing framework deliberately integrated rural crime monitoring into its national strategy, recognising that cyber-enabled fraud and financial scams often emanated from under-policed rural regions [38]. Similarly, in India, the National Digital Communications Policy (2018) incorporated rural digital crime prevention into its broader ICT expansion agenda, ensuring that rural areas were not treated as peripheral. Nigeria's failure to embed similar mechanisms indicates that its frameworks are not technologically deficient but politically selective.

The consequence of excluding rural digital forensic needs from policy frameworks is the creation of systemic blind spots in Nigeria's security architecture. Rural cases often collapse in court due to lack of forensic evidence, reinforcing a cycle of impunity. This not only undermines justice delivery for rural citizens but also weakens national resilience against cybercrime, as rural areas become safe havens for criminal activity or hideout. Furthermore, the absence of clear frameworks discourages international cooperation and donor support, as external partners find it difficult to align assistance with fragmented national priorities. To address this gap, Nigeria must reconceptualise its digital forensic frameworks to explicitly include rural realities. This requires three reforms: (1) decentralisation of policy design to ensure rural voices are represented; (2) establishment of inter-agency coordination mechanisms tailored for rural contexts; and (3) integration of rural digital forensics into broader cybersecurity and ICT strategies. Hence, without these systemic adjustments, Nigeria's frameworks will continue to reproduce inequality, leaving rural communities outside the scope of digital justice. In the same vein, despite Nigeria's adoption of several cyber-related laws, the legal framework for digital forensics remains underdeveloped and ambiguously interpreted. Key legislative instruments such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, the Evidence Act 2011, and the Administration of Criminal Justice Act (ACJA) 2015 offer only limited or inconsistent provisions regarding the collection, storage, and admissibility of digital evidence. Similarly, the 2011 Evidence Act, for instance, recognizes electronic evidence as admissible but provides limited guidance on chain-of-custody, authenticity verification, or metadata handling all of which are essential pillars in digital forensic procedures [39]. This ambiguity poses challenges not only in urban jurisdictions but particularly in rural settings where prosecutors and law enforcement officers may lack the specialized legal knowledge to navigate these complexities.

Moreover, according Okoro [39], added that many rural courts and magistrates have limited exposure to digital forensic principles. This leads to the outright rejection or misinterpretation of digital evidence during prosecution. As a result, criminals operating in rural communities especially in cases of terrorism, kidnapped hostage, cyberbullying, phone scams, or internet fraud are often released due to 'insufficient evidence,' even when incriminating digital traces exist. Furthermore, Germany's response to perceived weaknesses in

the legislative framework for digital evidence has been multi-pronged statutory refinement, technical standardisation, judicial oversight, and stronger public and private cooperation. Recent scholarship and practice show that Germany has anchored digital-evidence procedures in existing criminal-procedure law (StPO) while layering technical and organisational safeguards to preserve admissibility and integrity. The Code of Criminal Procedure now explicitly recognises electronic documents and provides procedural routes for their use in prosecutions, improving legal certainty for investigators and courts. (Federal Law Gazette, 2024) Furthermore, at the technical and operational level, the Federal Office for Information Security (BSI) has published IT-forensics guidance and standards that professionalise evidence collection, chain-of-custody documentation, and tool validation, helping to translate legal rules into reproducible practice for authorities and private experts. These BSI instruments function as de-facto quality control, reducing disputes over method and admissibility. While the Judicial review, especially by the Federal Constitutional Court, has been a crucial corrective high-profile ruling (e.g., decisions in 2020 and 2024) emphasised proportionality and data-protection limits on surveillance and evidence gathering, forcing legislators and agencies to narrow powers and adopt stricter safeguards. This jurisprudence elevated constitutional constraints into practical limits on investigative methods.

The European Parliament Migration and Home Affairs in her view for Cross-border evidence gaps were addressed through engagement with EU instruments and national adaptation to the e-evidence package (European production and preservation orders), which streamlined lawful access to provider-held data and clarified roles for courts and service providers reducing legal uncertainty in transnational cases. Therefore, the empirical and doctrinal studies conclude that the combination of codified procedure (StPO), binding technical standards (BSI), active constitutional review, and EU-level cooperation has substantially mitigated the "weak legislative framework" problem in Germany though authors still call for continuing refinement in oversight, transparency, and provider compliance mechanisms. Therefore, the absence of specialized cybercrime courts or dedicated digital evidence units in rural jurisdictions further compounds the problem, effectively disenfranchising rural communities from accessing justice through digital means. Hence, practical based approach is employed by the German government to mitigate this challenge.

2.9 Neglect of Rural Realities in National Policies

Digital forensic policies in Nigeria tend to be urban-centric, with little consideration for the distinct challenges of rural communities. National strategies such as the National Cybersecurity Policy and Strategy (NCPS) 2021 and Nigeria Digital Economy Policy and Strategy (2020–2030) emphasize capacity building, public-private partnerships, and ICT development. However, they rarely provide frameworks for addressing digital justice in rural communities or tailoring forensic tools to low-resource settings. The consequences of this neglect according to Oyedepo 2013 are multi-fold. Firstly, he added that rural officers are excluded from digital policy training programs and budgetary allocations for forensic capacity followed by little to no consultation with local actors during policy formulation, meaning rural realities such as low literacy rates, limited electricity, and infrastructural isolation are ignored.

Finally, according to Holt & Bossler, 2016; Burruss et al., 2019 in their views stated that policies often overlook traditional power structures and communal conflict resolution mechanisms that dominate rural areas. In some communities, cyber-related crimes are settled outside the formal justice system due to mistrust of state institutions or lack of prosecutorial pathways, reducing the incentive for digital evidence preservation altogether. This policy void ensures that rural areas remain peripheral to the national forensic agenda, reinforcing the digital divide and denying rural populations equal protection under the law. On a contrary, in

developed contexts such as Japan and China, the neglect of rural realities in national policy frameworks has been addressed through deliberate integration of rural-specific needs into broader development strategies. Japan, for instance, adopted the "One Village One Product" (OVOP) movement, which empowered rural communities to develop unique economic identities while receiving state support in marketing, infrastructure, and technology. This approach ensured that national modernization did not exclude rural populations but instead linked them to urban and global markets (Yamagami & Sato, 2020). Similarly, China has pursued the "Rural Revitalization Strategy," introduced in 2017, which explicitly recognized the infrastructural and digital disparities between rural and urban areas. The strategy emphasizes improved road networks, internet connectivity, and local governance reforms to ensure rural communities are not marginalized in the country's digital economy (Long et al., 2020). Both countries demonstrate that addressing rural neglect requires multi-sectoral investments spanning transport, digital infrastructure, and local empowerment while ensuring that rural development is not treated as peripheral but central to national progress. For Nigeria, such models highlight the importance of embedding rural realities in policy design to mitigate disparities in digital forensic deployment and other critical services.

2.10 Conclusion

These findings converge on a stark reality of while the urban Nigeria is advancing towards digital justice, her rural communities remain marginalized, creating a two-tiered investigative and justice system that jeopardizes national security particularly cybercrime response strategies. Hence, without decentralizing digital forensic infrastructure and investing in rural capacity, Nigeria risks deepening existing disparities in access to investigation, justice, undermining both citizen trust and national security efforts.

2.11 Summary

This chapter reviews academic and policy literature on digital forensic practice, identifying major themes such as infrastructure dependency, institutional readiness, training capacity, and policy frameworks. Particular attention is given to studies on developing countries, where structural inequalities mirror Nigeria's rural context. The review identifies significant research gaps especially the neglect of rural realities and infrastructural deficits in digital forensic studies. Recognizing these gaps underscores the importance of grounding the analysis in a suitable theoretical framework that can explain the socio-technical and institutional dynamics or challenges shaping forensic practice in rural Nigeria. This provides the rationale for chapter three.

3 Digital Forensic Challenges in Rural Nigeria

3.1 Introduction

Rural Nigeria faces significant barriers to effective digital forensic investigation. These include inadequate infrastructure (road network, power supply, internet, lab facilities), poor digital literacy, and lack of trained personnel. Case studies such as a 2020 incident in Benue State, where chat logs crucial to a sexual harassment case were lost due to improper evidence preservation, highlight the consequences of these limitations. The digital divide is stark, with urban centers advancing while rural communities remain technologically underserved. However, this chapter explores the key infrastructural limitations that hinder digital forensic effectiveness in Nigeria's rural communities. It is thematically organized around three key dimensions and three sub-categorized units corresponding to the study's first set of lower-level objectives: (1) Rural communities in Nigeria; overview (2) Infrastructural development in Nigeria's villages (3) Role of infrastructure in the effectiveness of digital forensic research. Sub-units (i) access to forensic technology and laboratories; (ii) digital connectivity and power supply; and (iii) rural law enforcement capabilities.

3.2 Rural Communities in Nigeria: Overview

National Bureau of Statistics, 2020 opined that rural communities in Nigeria like Amede, Umuleshia, Epkpeye, Olorinda, Sabon gari etc are typically characterized by low population density, limited access to social amenities, and a reliance on subsistence agriculture. While Aderibigbe & Olanrewaju, 2021 added that these areas often suffer from poor infrastructure, such as inadequate roads network, electricity, and internet connectivity, which hinders development and access to essential services. He maintained that the educational and healthcare systems are generally under-resourced, economic opportunities are limited, leading to high poverty rates while cultural practices and communal living remain strong, with traditional leadership structures playing significant roles.

Furthermore, rural communities in Nigeria are known for lower literacy rates and significant digital exclusion, limiting residents' ability to access technology, interpret, and benefit from digital information. According to the National Bureau of Statistics (2020), adult literacy rates in rural areas are markedly lower than in urban centres, with some northern rural states recording literacy levels below 30%. Digital exclusion is further entrenched by inadequate ICT infrastructure, high internet costs, and limited electricity supply, which restrict access to online education, e-government services, and digital marketplaces. For example, in rural parts of Enugu, Borno and Taraba States, intermittent network coverage and the absence of functional computer centres hinder residents' participation in Nigeria's growing digital economy (World Bank, 2021; International Telecommunication Union, 2020). Suffice to say, they are alien to infrastructural development as underscore in digital forensic inclusiveness.

3.3 Infrastructural Development in Rural Nigeria

Infrastructure refers to the fundamental physical, organizational facilities and systems necessary for the functioning of a society or enterprise Aderamo, & Magaji, (2010). It includes transportation systems (roads, bridges), communication networks, electricity, water supply, sanitation, schools, healthcare facilities, and digital connectivity. These systems are essential for economic development, social well-being, and the delivery of public services. Hence, Infrastructure in rural communities whether in developing nations like Nigeria or in advanced countries like the United Kingdom is not merely important but is critical for survival, socioeconomic progress, and integration into the national economy. In the Nigerian context, inadequate infrastructure such as poor road networks, unreliable electricity, limited potable water supply, and insufficient digital connectivity severely constrains access to essential services, including law enforcement and forensic investigations (World Bank, 2020). For instance, rural farmers in Benue State face post-harvest losses of up to 40% due to impassable roads that delay the transport of perishable goods to urban markets (FAO, 2019), a challenge that mirrors the logistical difficulties faced by rural police units attempting to transfer digital evidence to urban forensic laboratories. By contrast, in advanced economies such as Canada, targeted investments in rural broadband have facilitated access to telemedicine, e-learning, and e-commerce, narrowing the digital divide and strengthening community resilience (OECD, 2021). This illustrates that infrastructure functions both as a lifeline and an equalizer, directly influencing rural communities' capacity to participate in the national economy and to benefit from critical services such as digital forensic investigation. Nigeria's villages, however, infrastructure is not only insufficient but also unevenly distributed, presenting considerable challenges to digital forensic practice. Regrettably, the infrastructure in this context that can be classified into different categories based on their purpose and function still undermine digital forensic practice in Nigerian villages.

Firstly, physical infrastructure such as transportation networks and electricity supply is foundational yet notably inadequate in many rural regions. However, it refers to the fundamental facilities and systems necessary for the functioning of a society or enterprise,

including road networks, electricity grids, water supply systems, telecommunications, and buildings (Akinola & Olatunji, 2021). In support, Okoye et al., 2020 added that adequate physical infrastructure is critical for economic development, social inclusion, and access to essential services. But in Nigeria's rural areas, they are characterized by poor road networks which often hinder the transportation of digital forensic equipment and personnel to crime scenes, delaying investigations and reducing the integrity of evidence. Similarly, Ojo & Alabi, 2019 supported that poor road conditions and limited public transportation networks obstruct timely access to crime scenes and hinder the transfer of digital evidence to forensic laboratories. This assertion was again agreed by Eze & Adewale [40,41], in their views stated that during the rainy season, certain roads become entirely impassable, delaying investigations and risking evidence degradation. For instance, the delay and loss of evidence without backup or referral options while accessing Nigerian Police Digital Forensic Laboratory (NPDFL), based in Abuja from rural part of Nigeria was due to bad road network. In the same vein, they further added that inconsistent or nonexistent power supply across many rural communities renders forensic tools and devices inoperable as over 60% of rural communities in Nigeria like Amede, Umuleshia, and Epeye lacks reliable electricity, making it impossible to power forensic hardware, charge mobile devices, or run data recovery systems on-site. For example, the failure of 2022 online recorded fraud case perpetrated through mobile devices in a rural part of Ogun State illustrates the power supply deficiency in the area. Similarly, the longer it took to transport key evidence from rural to urban centres, recoded losses due to improper handling traced to lack of power supply and bad road network. This delay led to data bridge and distrust which prompted the dismissal of the case on technical grounds (Premium Times, 2022).

Secondly, Communication infrastructure is seen as an underlying physical and digital systems that enable the transmission of information, such as telecommunication networks, internet connectivity, mobile towers, satellite systems, and broadcasting facilities (Wikipedia). In rural Nigeria, inadequate communication infrastructure such as poor broadband penetration, unstable mobile networks, and lack of fibre-optic coverage significantly limits the capacity of law enforcement agencies to coordinate digital forensic investigations. For instance, in Borno State, limited mobile network reach means that investigative teams often rely on radio communication and physical dispatch of information, leading to delays in evidence transfer and case resolution (Oyedepo, 2021). This is equally deficient, particularly in areas such as broadband internet and mobile network coverage. While broadband penetration in urban areas exceeds 80%, rural regions remain under 30%, significantly limiting the availability of real-time digital evidence retrieval tools such as cloud data access or mobile device tracking (Nigerian Communications Commission [NCC], 2022). In the same vein, Ibrahim & Okoye, 2020; Sani & Musa, 2021 in their views stated that lack of reliable network coverage means that critical digital footprints such as call logs, social media interactions, and location data may be difficult or impossible to access during the crucial initial stages of investigation. For instance, during the 2019 gubernatorial elections in rural parts of Kogi State, several incidents of vote-buying and electronic ballot manipulation were reported. Despite numerous smartphone recordings made by citizens, local police could not preserve or transmit digital footage to the appropriate channel because of internet bridge. In some cases, the evidence was deleted due to lack of understanding of smart phone operations like cloud and other technical features in both Android and Apple phones or computer systems. Therefore, no forensic analysis was conducted, and cases were dismissed due to insufficient evidence (INEC Report, 2020).

Thirdly, Social infrastructure, in Afikpo, Ebonyi State, a 17-year-old boy faced cyberbullying from classmates who circulated deep-fake videos of him. His parents approached the police, who dismissed the matter as a "private dispute" with no criminal substance. The officers had no training in digital forensics or understanding of cyber harassment. The psychological

harm endured by the victim was significant, yet no justice was served (Chukwuemeka & Odili, 2022). No wonder Adrews 2020 sees social infrastructure as physical facilities, services, and networks that support the quality of life, social well-being and security of a community, enabling access to essential services such as education, healthcare, housing, recreation, and public safety. He added that the structures foster social inclusion, economic participation, and community cohesion. Chukwuma et al., 2020 narrowed it down as include the presence of well-equipped police stations, trained personnel, and forensic laboratories, though mostly concentrated in Nigeria's urban centers then the scarcity of forensic facilities in rural areas forces investigators to transport digital evidence over long distances, which not only increases investigation time but also heightens the risk of evidence contamination or loss. Furthermore, lack of training in digital evidence handling among rural officers as a social need, often leads to mishandling or outright loss of data, rendering evidence inadmissible in court [42].

Fourthly, digital infrastructure is seen as the foundational technological systems and resources that support the creation, storage, processing, transmission, and exchange of digital data and services. It includes physical components such as data centers, servers, fiber-optic cables, and undersea cables, as well as virtual systems like cloud computing platforms, software frameworks, and network architectures that enable seamless digital connectivity and service delivery (Katz et al., 2021). But in Nigeria's particularly the rural communities as Ogunleye & Adebayo, 2022 stated, is either those technologies are outdated or completely lacking in most rural Nigerian police units. This technological gap makes it nearly impossible to conduct onsite data recovery or forensic analysis, which are critical in preserving volatile digital evidence. Compounding this issue is the limited availability of structured digital forensic training, resulting in inadequate skills among law enforcement officers to utilize such tools even when available (Ekwueme & Nwosu, 2021).

Fifthly, economic Infrastructure is a basic physical and organizational structures, facilities, and systems that support productive economic activity and enable the functioning of markets. It includes transport networks (roads, railways, ports, airports), energy supply systems (electricity generation and distribution), water supply, irrigation facilities, telecommunications, and other utilities that facilitate trade, production, and investment. Strong economic infrastructure reduces transaction costs, improves efficiency, and stimulates economic growth by enabling businesses, industries, and households to operate effectively (Calderón & Servén, 2010). In support of the above definition, Afolayan & Okeke, 2022 stated that funding mechanisms, logistics, and procurement channels significantly impacts forensic capacity. Rural police units and local governments often lack budgetary provisions to maintain forensic tools or secure digital infrastructure. This results in a heavy dependence on external agencies, delayed procurement processes, and limited logistical support for transporting evidence and personnel. Where vehicles, storage facilities, or secure evidence lockers are unavailable, the integrity and chain-of-custody of digital evidence are often compromised. Consequently, the lack of integrated and functional infrastructure spanning physical, digital, communication, social, and economic domains severely undermines the ability to conduct effective digital forensic investigations in rural Nigeria. Each deficiency amplifies the others, forming a systemic bottleneck that prevents timely, accurate, and legally sound digital investigations which can further be illustrated in summary example and case studies from rural Nigeria below:

Benue State: Sexual Violence Case Dismissed
ECOWAS Court dismisses sexual violence case against Nigeria, citing insufficient digital forensic evidence to support claims of sexual violence, denial of reproductive rights, and lack of access to justice as filed by a Nigerian citizen from Benue State, who alleged multiple violations of her fundamental rights following a sexual assault she suffered as a minor in

part of Abuja. (Premium Times, 2025). In the same vein, a 2022 case in Guma LGA, Benue State, involved the digital sexual harassment of a teenage girl via WhatsApp. Local police were ill-equipped to preserve or extract the chat logs from the suspect's phone before it was reset. The digital evidence was lost, and no charges were filed due to insufficient admissible proof (Daily Trust, 2022).

Kano State: Teenage Girl Blackmail Opted
A 2021 case in rural Kano involved a teenage girl blackmailed through manipulated photos shared online. The victim's family opted to resolve the issue through a local religious leader instead of involving law enforcement, leading to the suspect going unpunished (Premium Times, 2021).

Abuja-Kaduna Train Attack: Victims kidnapped into the forest
Also, the ISWAP terrorists and kidnappers seen in a viral video on Facebook beating the remaining of Abuja-Kaduna train kidnaped victims to send a warning to Buhari led government. The captives were held in the bush for over 3 months unchallenged by the law enforcement agencies (Omobola, 2022).

Zamfara State: Mistaken Military Airstrike
Again, at least 16 civilians in Nigeria's north-western Zamfara State have been killed in a military air strike, apparently after being mistaken for criminal gangs. Residents told local media the victims were members of local vigilante groups and civilians defending themselves from armed gangs notorious for kidnapping people for ransom. In the same vein, in 2023, at least 85 civilians, mostly women and children, attending a Muslim religious gathering at a village in Kaduna state were killed after they were mistaken for bandits (BBC News 2025).

This illustrates how infrastructure deficiencies at multiple levels hinder digital forensic effectiveness in rural Nigeria. Therefore, the practice of digital forensics in the place is critically important for contemporary justice delivery. While urban areas are gradually adapting to digital methods of crime investigation, rural communities remain sidelined due to infrastructural, educational, and policy limitations. The result is a dualistic justice system where technology empowers some while disenfranchising others. Bridging this gap requires a coordinated national effort to decentralize digital forensic infrastructure, physical basic amenities, build capacity in rural law enforcement, and increase digital literacy among rural dwellers. Only then can the benefits of digital justice be equitably distributed across Nigeria.

3.4 The Role of Infrastructure in the Effectiveness of Digital Forensic Research

The effectiveness of digital forensic research as may be viewed world over, is largely dependent on the availability and quality of key infrastructure. Therefore, infrastructure in this context extends beyond physical laboratories to encompass hardware, software, networks, skilled personnel, and institutional frameworks that enable secure acquisition, preservation, analysis, and presentation of digital evidence. This means that without robust infrastructure, the quality, speed, and admissibility of forensic outputs are significantly undermined. However, at the most fundamental level, physical and logical infrastructure provides the secure environment necessary for handling sensitive evidence as properly designed forensic laboratories, with features such as controlled access, climate regulation, surveillance systems, and tamper-proof storage, are crucial in maintaining evidential integrity and ensuring compliance with chain-of-custody standards (CACI, 2023). Similarly, high-performance forensic workstations, servers, and data storage systems, supported by reliable and segmented networks, are indispensable for processing the ever-growing volumes of digital data generated

in investigations.

Furthermore, scalability also plays a vital role in forensic effectiveness, including explosion of digital devices and storage capacities that have created unprecedented data backlogs in many forensic units worldwide. In the same vein, research indicates that automation and server-based orchestration frameworks can reduce these delays by running 24/7 evidence processing cycles and allowing scarce human expertise to focus on complex analytical tasks (Baar, Alink, & Beek, 2017). Such scalable infrastructure ensures that research output remains timely and relevant, even in the face of increasing investigative demand. Equally important is the interoperability and standardization of forensic tools viewed from the absence of uniform validation frameworks and benchmarking datasets that hinder reproducibility and comparative analysis, which are cornerstones of credible infrastructural research. For instance, the accreditation schemes such as ISO/IEC 17025, alongside collaborative initiatives like the European Network of Forensic Science Institutes (ENFSI), provide models for harmonizing methods and ensuring that findings are scientifically defensible and admissible in court (Parliament UK, 2019). This underscores how infrastructural alignment contributes directly to the credibility of digital forensic research. Similarly, the rapid adoption of cloud computing therefore presents both opportunities and challenges for digital forensics. On the one hand, frameworks such as Digital Forensics as a Service (DFaaS) provide scalable, distributed platforms for handling complex investigations remotely. On the other, cloud environments complicate evidence acquisitions due to jurisdictional constraints, data dispersion, encryption, and multi-tenancy issues (Ruan, Carthy, Kechadi, & Crosbie, 2011; Zawoad & Hasan, 2013). Without infrastructure that supports hybrid or cloud-ready forensic investigations, research risks lagging technological realities. By implication, infrastructure also extends to human capital this includes skilled forensic experts, equipped with both technical and legal competencies, are essential for interpreting evidence and adapting methodologies to emerging technologies. However, many jurisdictions face shortages of trained personnel, resulting in investigative delays and limited research innovation (IntechOpen, 2021). Therefore, investment in training facilities, knowledge transfer, and continuing professional development is as critical as investment in hardware or software. Finally, resilient infrastructure often requires partnerships between public agencies, private providers, and academic institutions. While outsourcing certain tasks to accredited private laboratories can relieve backlogs, inconsistent use of external services and concerns about cost or quality can undermine effectiveness (HMICFRS, 2022). A coordinated national strategy that balances internal capacity with external partnerships strengthens resilience and enhances the reliability of forensic research.

Digital forensic research, therefore, cannot thrive in environments where infrastructure is inadequate, fragmented, or outdated. From secure laboratories and scalable hardware to standardized tools, cloud-ready frameworks, skilled personnel, and strategic partnerships, infrastructure forms the backbone of effective forensic practice worldwide. Investments in these areas not only enhance the speed and quality of research but also ensure that digital evidence remains credible, admissible, and impactful in the pursuit of present justice system. Contrarily, in Nigeria's rural communities, systemic infrastructural deficiencies pose major obstacles to effective digital evidence acquisition, handling, analysis, and prosecution. Though the urban centres enjoy relative benefits of forensic laboratories, reliable internet, electricity, and trained personnel, rural areas remain under-resourced and disconnected from these critical components.

3.4.1 Unit i: Limited Access to Forensic Infrastructural Technology and Laboratories

The advancement of forensic investigation relies heavily on the availability and accessibility of modern infrastructural technology and specialized laboratories. These facilities provide

the technical foundation necessary for the collection, preservation, and analysis of digital evidence in criminal justice systems. However, in many developing contexts, particularly Nigeria, access to such forensic-enabled infrastructure remains severely constrained, limiting the effectiveness of digital forensic investigations.

One of the core challenges is the insufficient number of functional forensic laboratories. While developed countries have established multiple regional forensic centers equipped with advanced technologies such as DNA sequencing, digital imaging, and cyber forensic units, Nigeria and other African states struggle with only a handful of under-resourced laboratories [43]. For example, most Nigerian police formations lack dedicated cybercrime laboratories, forcing investigators to rely on overstretched national facilities in Abuja or Lagos (Olagunju & Oladipo, 2020). He added that this concentration of infrastructure in urban centers creates an imbalance that sidelines rural communities where digital crimes also occur. Furthermore, another dimension of the problem is the technological gap largely seen in forensic investigation today which requires high-level tools such as mobile forensic devices, computer imaging systems, network traffic analyzers, and malware detection platforms (Casey, 2019). Yet, most Nigerian law enforcement agencies cannot afford these technologies due to budgetary constraints and lack of consistent government investment (Ogunleye & Ojedokun, 2021). This means that even when crimes involving digital evidence are reported, investigators may not have the equipment to extract or preserve data in a manner admissible in court.

Akinyemi & Adeoye, 2022 stated that infrastructural limitations are also linked to power supply and internet connectivity. He maintained that reliable electricity and broadband networks are essential for the operation of forensic laboratories and digital evidence storage systems. However, persistent energy shortages and poor ICT infrastructure across much of rural Nigeria weaken the capacity of forensic institutions to function effectively. Without stable electricity, sensitive forensic equipment risks frequent breakdowns, while poor connectivity hinders remote access to international databases used for criminal investigations. Furthermore, the absence of adequate collaboration between public and private forensic institutions aggravates limited access. In countries like South Africa and India, public-private partnerships have helped expand laboratory services and integrate cutting-edge forensic technologies into the justice system (Chisum & Turvey, 2019). In contrast, Nigeria's forensic sector remains fragmented, with private laboratories often working in isolation and without formal links to law enforcement (Olayemi, 2020). This disjointed structure reduces opportunities for resource sharing and capacity building.

Summarily, limited access to forensic-enabled infrastructural technology and laboratories in Nigeria reflects a combination of inadequate facilities, underfunding, weak rural coverage, unreliable utilities, and insufficient human capital. These constraints not only weaken the ability of investigators to collect and analyze digital evidence but also undermine the credibility of evidence presented in courts. Addressing these challenges will require a multi-stakeholder approach involving government, academia, and the private sector to ensure equitable access to modern forensic infrastructure across both urban and rural contexts. This can be further viewed in some developed countries such as the United Kingdom, the United States, and China that have made significant investments in forensic-enabled infrastructural technology and laboratories, creating advanced systems that serve as global benchmarks for scientific investigation. These infrastructures integrate both traditional and digital forensic capabilities, ensuring accuracy, reliability, and efficiency in the justice system. In the United Kingdom (UK), forensic laboratories are characterised by innovation and robust infrastructure designed to support both research and law enforcement. The Cranfield Forensic Institute, inaugurated in 2021, represents a "centre of excellence" for forensic science, equipped with cutting-edge simulation environments for crime scene reconstruction,

digital forensic facilities, and virtual autopsy tables (Cranfield University, 2021). Similarly, the South Wales Joint Scientific Investigation Unit (SWJSIU) houses specialised laboratories for ballistics, trace evidence, and fingerprint analysis, alongside unique technologies such as a metal vacuum deposition facility used to recover fingerprints from smooth surfaces (South Wales Police, 2012). In the digital domain, the UK has strengthened infrastructure through accredited laboratories like CACI's Digital Forensics Lab, which provides ISO/IEC 17025:2017-compliant digital forensic services to law enforcement (CACI, 2023). Private laboratories, such as the Computer Forensics Lab in London, further enhance national capacity by offering secure environments for mobile devices, cloud, and memory forensics (Computer Forensics Lab, 2022). Importantly, the UK also maintains governance frameworks such as the Biometrics and Forensic Ethics Group, which ensures ethical compliance in the deployment of biometric and forensic technologies (Home Office, 2020).

Similarly, the United States (US) possesses some of the most advanced forensic infrastructures worldwide, centred on large federal and regional facilities. The Federal Bureau of Investigation (FBI) Laboratory at Quantico stands as one of the largest and most sophisticated forensic laboratories globally, providing comprehensive services in DNA analysis, digital evidence, toxicology, and trace materials, while supporting all levels of law enforcement (FBI, 2021). Complementing this, the Regional Computer Forensics Laboratory (RCFL) network provides specialised hubs for digital investigations, data recovery, and training, enabling the FBI and local agencies to process thousands of digital evidence cases annually (Noblett et al., 2000). Infrastructure development in the US is guided by scientific standards, including the National Institute of Standards and Technology's (NIST) Handbook for Forensic Science Laboratories, which provides detailed guidance on laboratory planning, facility design, and technological upgrades (NIST, 2013).

Furthermore, China's forensic infrastructure has expanded rapidly over the last two decades, combining state-led investment with accreditation frameworks and technological innovation. By 2023, China had established 18 virtual autopsy laboratories across 13 provinces, supported by digital imaging, three-dimensional reconstruction, and minimally invasive forensic tools, with plans for further expansion (Zhang et al., 2024). Following the 2005 "2.28 Decision," accreditation became mandatory for forensic institutions, requiring compliance with ISO/IEC 17025 and other national standards, thereby ensuring credibility in evidence handling (Li & He, 2018). By 2018, over 100 digital forensic organisations had received accreditation, and more than 370 forensic science standards had been developed across disciplines such as toxicology, trace evidence, and document examination (Houck, 2018). In a view of Shanghai Daily, 2016 opined that regional laboratories, such as those in Shanghai, have built extensive DNA databases with over one million profiles, supported by contamination-controlled environments. More recently, China has pioneered artificial intelligence applications in forensic medicine. For example, the Forensic Evidence Analysis Transformer (FEAT), introduced in 2025, leverages large language models to assist medicolegal experts in cause-of-death analysis, marking a new phase in AI-enabled forensic infrastructure (Li et al., 2025).

Therefore, developed countries have established forensic laboratories both in urban and rural areas, that not only embody advanced scientific and technological capabilities but also reflect strong accreditation, governance, and innovation frameworks. The UK prioritises balanced integration of public and private forensic services with ethical oversight, the US emphasises national coordination through large federal and regional labs, while China focuses on rapid expansion, accreditation, and the adoption of AI-enabled forensic technologies. These infrastructures provide valuable models for developing nations like Nigeria seeking to strengthen their forensic science ecosystems.

3.4.2 Unit ii: Poor Digital Connectivity and Unstable Power Supply

One of the most pressing challenges facing digital forensic investigation in Nigeria's rural communities is the problem of poor digital connectivity and unstable power supply. Effective digital forensic processes rely heavily on infrastructure such as high-speed internet, secure data transmission systems, and consistent electricity to ensure that evidence can be collected, analyzed, and stored in a timely and legally admissible manner (Casey, 2019). Unfortunately, rural areas in Nigeria are characterized by significant infrastructural gaps in these two domains, which hinders the full deployment of digital forensic services and compromises justice delivery.

a) Poor Digital Connectivity

Reliable internet connectivity is indispensable for modern digital forensics because it supports remote investigations, facilitates data transfer, enables access to digital forensic tools stored on cloud platforms, and allows real-time collaboration between investigators across jurisdictions (Gogolin, 2010). In Nigeria, however, digital connectivity is largely concentrated in urban centres such as Lagos, Abuja, and Port Harcourt, while rural areas remain underserved. The Nigerian Communications Commission (NCC) reports that although broadband penetration in Nigeria reached over 50% in 2023, coverage in rural communities remains far below the national average, with some areas experiencing less than 15% penetration (NCC, 2023). This digital divide significantly affects the ability of rural law enforcement agencies to use digital forensic technologies. Olayemi, 2014 in his view supported that the lack of reliable digital connectivity in rural communities also contributes to delays in the processing and transmission of digital evidence. For example, forensic laboratories often require large volumes of data to be transferred from the crime scene to a central facility for analysis. Without strong internet infrastructure, evidence may need to be transported physically, which increases risks of data corruption, tampering, or loss. In addition, weak connectivity restricts rural investigators from using advanced cloud-based forensic tools, which are becoming the global standard due to their scalability and efficiency (Raghavan, 2013). This widens the technological gap between Nigeria's rural investigators and their counterparts in more developed or urbanised regions. Moreover, poor connectivity according to Volonino & Anzaldua, 2008 undermines the principle of chain of custody, which requires that digital evidence remains intact and verifiable from the moment it is collected until it is presented in court. Interruptions in data transmission caused by weak connectivity can lead to incomplete logs, data inconsistencies, or even inadmissibility of evidence in legal proceedings. Thus, while urban investigators may leverage advanced forensic platforms to maintain integrity, their rural counterparts remain at a disadvantage due to infrastructural inadequacies.

b) Unstable Power Supply

Closely linked to the challenge of poor connectivity is the issue of unstable power supply. Reliable electricity is critical for powering forensic laboratories, servers, storage devices, and other essential ICT infrastructure. However, Nigeria's power sector remains plagued with inefficiency, with national generation averaging less than 5,000 megawatts for a population of over 200 million people (Oyedepo, 2022). Rural areas bear the brunt of this crisis, as they often face longer power outages, lower grid coverage, and over-reliance on alternative sources such as diesel generators and solar panels (Adenikinju, 2020). Consequently, this deters forensic investigations' highly power-dependent processes including digital evidence, that would be once acquired, must be stored in secure servers that require uninterrupted electricity to prevent data loss or corruption. Power interruptions during evidence imaging or analysis can lead to incomplete or damaged datasets, compromising the reliability of forensic outcomes (Reith, Carr, & Gunsch, 2002). Similarly, forensic laboratories depend on high-capacity computing systems to run specialised software for tasks such as file carving, malware analysis, and network traffic reconstruction. Without stable electricity, these pro-

cesses are frequently disrupted, leading to significant delays in investigations and judicial proceedings. And the reliance on backup generators in rural areas according to Oyedepo 2012 also presents challenges. He added that generators are expensive to acquire and maintain, particularly for underfunded police stations and local forensic units if any. He further stated that the noise, fuel shortages, and environmental hazards associated with generators make them unsustainable for long-term digital forensic operations. While renewable energy sources such as solar power offer potential alternatives, their deployment in forensic environments requires high upfront investment and technical expertise that rural communities often lack.

c) Interconnected Challenges

The combined effect of poor digital connectivity and unstable power supply creates a vicious cycle that undermines forensic capacity in rural Nigeria. For example, even where satellite internet services are available, they cannot function optimally without stable electricity to power routers, modems, and computing devices. Similarly, forensic equipment such as mobile extraction kits and imaging devices relies on both electricity and connectivity to operate effectively. The lack of synergy between these infrastructures means that rural forensic investigators often face systemic limitations that urban investigators do not encounter (Eze, 2021). From a broader perspective, these infrastructural deficiencies perpetuate the marginalisation of rural populations in access to justice. Digital evidence is increasingly central to the prosecution of crimes ranging from cyber fraud to terrorism. When rural communities cannot effectively collect and present such evidence due to infrastructural deficits, criminals operating in these regions enjoy a 'de facto' immunity, further eroding trust in the justice system (Chisum & Turvey, 2011). Poor digital connectivity and unstable power supply, therefore, represent critical obstacles to effective digital forensic investigation in Nigeria's rural communities. These infrastructural deficits not only delay investigations but also compromise the integrity, admissibility, and timeliness of digital evidence. Addressing these challenges requires a coordinated national strategy that invests in rural broadband expansion, strengthens the national grid, and promotes renewable energy solutions tailored to forensic operations. Without such interventions, rural Nigeria will remain disadvantaged in the digital forensic landscape, thereby perpetuating the urban-rural divide in justice delivery.

3.4.3 Unit iii: Inadequate Technical Capacity and Support in Rural Law Enforcement

The shortage of skilled digital forensic personnel in Nigeria's rural communities is frequently presented as a matter of insufficient training opportunities. While this diagnosis is partly correct, a deeper analysis reveals that the issue is rooted in structural imbalances in education, governance, and professional incentives. Rural law enforcement officers are not only undertrained but are also embedded in systems that discourage retention of forensic expertise, even when training is available. At a descriptive level, most forensic training facilities are concentrated in Nigeria's urban centres, such as Lagos and Abuja, making access difficult for officers in rural postings (Ogunleye & Adekunle, 2020). However, the concentration of training in cities is not accidental; it reflects an urban-centric security strategy that assumes cybercrime and digital evidence needs are primarily urban phenomena. This perception blinds policymakers to the reality that rural communities are increasingly exploited as staging grounds for cyber-enabled crimes, including mobile money fraud, online radicalisation, and telecommunications scams. By neglecting rural training needs, Nigeria effectively entrenches a two-tier forensic capacity system, urban areas with at least partial competence and rural regions with near-zero capacity. Even where rural officers gain exposure to training, poor incentives undermine retention. Many trained personnel are quickly transferred to urban centres where resources and career prospects are better, leaving rural commands in a perpetual cycle of skill drain (Okoro, 2021). This highlights a critical insight: the issue is not just training scarcity, but the failure of institutional structures to motivate, retain, and

professionalise rural forensic practice. Without addressing the broader conditions of rural policing-poor pay, inadequate housing, lack of recognition, training programmes risk becoming stop-gap measures that fail to build sustainable capacity.

Close evidence reinforces this point. In South Africa, the government partnered with universities to embed forensic training into police education, while offering financial and career incentives for officers to remain in rural postings [45]. Similarly, in Ghana, digital forensic capacity was decentralised by equipping regional police academies, rather than centralising all expertise in the capital (Asante, 2020). Nigeria's continued reliance on centralised, short-term training initiatives suggests a lack of political will to replicate such decentralised models.

The broader consequence of failing to develop rural forensic expertise is a widening justice gap. Rural communities remain unable to investigate or prosecute cyber-enabled crimes, resulting in cases being abandoned, misclassified, or transferred to urban jurisdictions with already overstretched resources. This not only erodes public trust but also creates spaces of impunity where criminal networks thrive. In the long term, the lack of skilled rural personnel undermines Nigeria's national cybercrime strategy, which depends on coordinated intelligence flows across both urban and rural policing structures.

Therefore, the challenge of skilled personnel in rural Nigeria cannot be reduced to training availability. It must be reframed as a systemic governance problem requiring integrated solutions, decentralised training institutions, professional incentives to retain rural officers, and career structures that value rural forensic practice equally to urban deployments. Without such reforms, training interventions will remain superficial, failing to address the root causes of rural forensic skill shortages.

Additionally, Adegoke & Okon, 2020 supported that even where minimal infrastructure exists, the effectiveness of digital forensic investigation is constrained by limited technical capacity among rural law enforcement officers. Most rural police personnel lack formal training in digital evidence preservation, cybercrime investigation, and the use of forensic tools. This results in procedural errors such as improper seizure of devices, failure to maintain chain-of-custody documentation, or contamination of evidence. Hence, the absence of technical support and mentorship from ICT professionals further deepens the problem. Unlike urban units that can call upon in-house forensic experts or contract private firms, rural stations often operate in isolation. As a result, potential digital evidence is frequently overlooked, discarded, or mishandled, especially in cases involving cyberstalking, financial fraud, or digital harassment. Institutional barriers are further illustrated where many rural command structures lack dedicated cybercrime desks or forensic liaison officers, meaning that even when evidence is preserved, there is no streamlined process to transfer or interpret it. This reinforces the cycle of investigative failure and erodes public trust in law enforcement capacity.

3.5 Conclusion

Strengthening digital forensics practice in rural Nigeria reviewed a pivotal role in modern investigative processes by enabling the identification, preservation, and analysis of digital evidence critical to criminal justice systems. In Nigeria, where cybercrime and digitally facilitated offenses are on the rise, the relevance of forensic technology is undisputed. However, the country's rural communities remain largely excluded from these advancements, due to systemic infrastructure deficiencies including centralized governance structures, lack of trained local personnel, legal illiteracy, and underdeveloped investigative frameworks.

3.6 Summary

Here, the study adopts a conceptual lens drawing from socio-technical systems theory and institutional theory to frame how digital forensic limitations in rural communities can be systematically analysed. The framework enables the study to move beyond surface-level descriptions of challenges and instead interpret them as interconnected issues of infrastructure, governance, and human capital. Therefore, with this framework established, the study then turns to the empirical realities of Nigeria's rural forensic landscape and comparative perspective and case studies from other developing countries which are explored in detail in chapter four.

4 Comparative Perspectives and Case Studies

4.1 Introduction

Comparative case studies are often used to suggest that Nigeria can learn from the successes of other developing countries in strengthening rural digital forensic capacity. While such comparisons are valuable, a deeper analysis shows that not all foreign strategies are transferable, given Nigeria's unique governance, infrastructural, and security contexts. The task, therefore, is not simply to replicate external models but to critically evaluate which elements can be adapted and which require context-specific modification. Therefore, some developing countries that have faced and addressed similar challenges to those confronting Nigeria in its rural digital forensic landscape are selected as follows India, Kenya, Brazil, South Africa, and Philippines which demonstrated innovative approaches to decentralization, public-private partnerships, community engagement, and training investments that offer practical lessons for Nigeria. By examining their strategies, the chapter identifies pathways that can be adapted and applied within Nigeria's rural law enforcement and digital forensic systems which may tailor its approach to local realities (Mwangi et al., 2022).

4.2 India: Decentralized Cyber Forensics and Regional Capacity Building

India provides one of the most cited examples, having addressed rural forensic gaps through mobile digital forensic laboratories deployed across states [46]. These labs improved evidence collection in remote areas where permanent facilities were unfeasible. However, in Nigeria, the feasibility of this model is questionable. Insecurity on highways and frequent attacks on police convoys raise significant risks for mobile labs carrying sensitive technology. This suggests that while the principle of decentralisation is useful, Nigeria may need to explore stationary regional forensic hubs rather than highly mobile units. Furthermore, India's vast geography and rural demographics mirror Nigeria's diversity and infrastructural imbalance. Recognizing this, India has developed regional cybercrime labs and digital forensic centres under the National Cyber Crime Reporting Portal and Indian Cyber Crime Coordination Centre (I4C). These regional hubs are equipped to support rural policing units with real-time digital evidence analysis and case management tools (Reddy & Patel, 2021). Similarly, India also partnered with local universities and police academies to offer regular digital forensics training to law enforcement officers. Mobile forensic kits are distributed to rural stations, enabling field-level data acquisition and secure evidence handling. These measures have significantly improved case turnaround time and digital evidence admissibility in rural jurisdictions.

In the same vein, India, with over 65% of its population residing in rural areas, has long recognized the limitations of handling digital crimes solely from urban centres. Rural India, like Nigerian villages, faces difficulties in reporting, investigating, and resolving cybercrimes due to the centralization of forensic capacity and the limited availability of digital investigation tools in non-urban settings. To address this, India launched decentralized District Cyber

Crime Cells, which serve as first responders to digital crime in semi-urban and rural districts. These cells are equipped with basic mobile forensic tools, while rural officers undergo digital investigation training through partnerships with institutions like the Indian Institute of Forensic Science. In parallel, the Cyber Hygiene for All initiative was introduced to promote public awareness on digital evidence preservation and cyber safety. India's cybercrime reporting portal, Cybercrime.gov.in, and SMS-based reporting options ensure accessibility for rural populations lacking reliable internet. The impact created therefore contributed to a 43% increase in rural cybercrime reporting and a doubling of conviction rates between 2018 and 2021 [47]. In the same vein, Nigerian government can draw a lesson from the above initiative by establish rural cybercrime desks within state police structures, provide digital forensic training to Divisional Police Officers (DPOs), launch public awareness programs using radio, SMS, and regional languages, and establish forensic outreach and helplines accessible via basic phones.

4.3 Kenya: Decentralisation, Public-Private Collaboration and ICT Integration

Kenya adopted a decentralised budgetary system that allowed counties to co-fund digital policing initiatives, ensuring rural communities had some level of forensic coverage (Mutua, 2021). This reduced dependence on central government and encouraged local ownership. Nigeria, however, operates a highly centralised fiscal system where states and local governments have limited financial autonomy. Replicating Kenya's model without constitutional reform would therefore be difficult. The key lesson here is the importance of fiscal decentralization but in Nigeria, this would require broader governance restructuring beyond the forensic sector. Detailed analysis revealed that Kenya has made notable strides in leveraging public-private partnerships to support rural forensic investigations. Through collaborations with firms such as Safaricom and local tech incubators, the Kenyan government has deployed digital evidence collection tools and training programs tailored for rural law enforcement (Wanjiru, 2022). He added that community awareness campaigns have also been critical in sensitizing rural populations on digital crime reporting, and improve Kenya's model emphasizes low-cost ICT solutions, including SMS-based complaint platforms and remote forensic support via mobile apps. These initiatives have improved trust in rural law enforcement and facilitated faster forensic responses.

In a similar development, Kenya invented Community Policing and Local Tech Hubs which helped the rural counties such as Turkana and Baringo changed the lack consistent electricity, digital access, and technical personnel a scenario that mirrors Nigeria's rural regions. Kenya in her innovative strategy, addressed this gap through Public-Private Partnerships (PPP) partnerships between government entities and tech hubs like iHub Nairobi and Tunapanda Institute. These collaborations produced Community Digital Responders (CDRs), and the local tech-savvy volunteers trained to assist police in digital evidence preservation. Additionally, mobile forensic kits were supplied through a partnership with the UK's Foreign, Commonwealth & Development Office (FCDO), enabling rural police to undertake tasks such as metadata recovery and chat log preservation. The Case Example in 2021, a sextortion case in Kajiado County led to a conviction after a CDR helped preserve WhatsApp messages, which were admitted as evidence in court (Njuguna & Otieno, 2022) further illustrate the impact that as Kenya's model improved up to a 30% increase in rural digital case resolutions between 2019 and 2022 (KICTANet, 2023). This is a necessary take home for Nigeria to partner with Nigerian tech hubs like Co-Creation Hub (Lagos) and Roar Nigeria Hub (Nsukka), train the rural youth as forensic first Responders and involve telecom companies through CSR programs to support rural digital justice.

4.4 Brazil: Digital Justice Inclusion and Localized Infrastructure

Brazil responded to geographic and infrastructural challenges by investing in satellite technologies, drone-assisted surveillance, and cloud-based forensic platforms (Silva & Ramos, 2019). This innovation bypassed weak transport and communication infrastructure. For Nigeria, such technologies appear attractive, but their success would depend on solving two structural problems including unreliable internet connectivity in rural areas and the vulnerability of digital platforms to corruption and misuse. Without reforms in governance and infrastructure, Brazil's high-tech solutions may collapse under Nigeria's current conditions. Again, the 'Justice on the Streets' (Justiça Itinerante) initiative enables mobile forensic teams to travel to rural and underserved areas. These mobile units, equipped with digital labs and trained personnel, conduct on-the-spot evidence analysis, offer legal consultations, and process cybercrime reports (Martins & Silva, 2020). Brazil has also localized data processing capabilities by establishing state-level digital forensic centres, reducing dependence on federal hubs. This decentralized model has enhanced rural access to forensic justice while preserving the integrity of the evidence chain.

Moreover, Brazil equally established a State-Level Digital Forensic Labs in Remote Provinces. This federal system initiative in vast rural provinces, particularly in the Amazon and northeast, which present geographical and logistical challenges like rural Nigerian states such as Taraba or Cross River was bridged through Brazil's Secretariat of Public Security that mandated the setup of digital forensic labs in each state capital. These were complemented by Mobile Digital Response Teams that provide services to remote municipalities including secure evidence storage, imaging software, and dedicated digital crime kiosks in rural towns. The impact according to a University of São Paulo evaluation (2020), the reforms led to a 60% reduction in rural cybercrime investigation timelines, strengthened community trust in local law enforcement and enhanced coordination between military and civil police forces. The Nigerian government from this initiative encourage state-level governments to fund and host digital forensic labs, develop mobile forensic teams targeting underserved rural LGAs and integrate rural forensic labs with state judiciary systems for rapid case processing.

4.5 South Africa: Training and Community-Led Forensic Outreach

South Africa focuses on community-driven approaches to rural digital justice. Through the Cybercrimes Act and funding from the Department of Justice, training modules on cybercrime reporting and digital evidence handling are integrated into rural policing curricula [48]. Importantly, South Africa promotes forensic literacy through rural community workshops, delivered in local languages. These initiatives encourage digital crime reporting, reduce stigma, and strengthen partnerships between police and communities which led the specialized rural cybercrime desks to pilot in provinces like Limpopo and Eastern Cape earlier faced with increasing digital victimization and limited police infrastructure like Nigeria's customary justice systems into a more inclusive digital forensic development. The Integrated Rural Justice Project (IRJP), backed by the National Prosecuting Authority and EU funds, embedded digital forensic specialists within local justice structures. The initiative equipped each district with a Mobile Forensic Van, conducted community sensitization programs on digital rights, and built working relationships between local chiefs and cybercrime units. Eurojust Strategy on Cooperation with International Partners (2024–2027). This results in over 1,000 rural digital victims assisted within 18 months, customary courts began issuing protective orders based on mobile phone evidence, and digital procedures were formally introduced into local dispute mechanisms (IRJP Report, 2022). Nigeria therefore can draw a lesson of collaborating with traditional justice systems to integrate digital forensics, deployment of mobile forensic units to complement rural court sessions and raise digital rights awareness in regions with high customary court reliance, such as the Middle Belt especially Benue State.

4.6 The Philippines: Adaptive Legal Frameworks and NGO Partnerships

The Philippines offers insights into legal adaptation and grassroots innovation. Recognizing the urban-rural divide, the government has decentralized certain cybercrime investigation functions to local police units while maintaining central oversight (Dela Cruz, 2022). However, civil society organizations play a major role in training local officers, monitoring forensic practices, and ensuring transparency, while mobile digital forensic kits, open-source software, and regional training centres made rural policing more responsive and aligned with global forensic standards.

The initiative further established USSD-Based Crime Reporting for Remote Islands that faced similar barriers as Nigeria's remote Local Government Areas poor connectivity, absence of internet services, and minimal law enforcement presence. The digital innovation of "TextJustice" platform enables USSD and SMS-based crime reporting. By implication, the local residents can submit incident codes, track case updates, and receive feedback via text. The installation of the Solar-powered kiosks by the Cybercrime Investigation and Coordinating Center (CICC) supports education and digital evidence collection in remote Barangays (villages). This impacted between 2021 and 2023, the system recorded over 12,000 rural complaints and supported the first rural cybercrime conviction in Palawan (CICC, 2023). Lessons for Nigeria will aid to develop multilingual USSD-based reporting systems (e.g., Igbo, Hausa and Yoruba), install solar-powered kiosks for digital awareness and reporting in unconnected areas and integrate reports into NPF's digital crime management system via collaboration with NITDA.

On the other hand, China integrated rural cybercrime prevention into its national digital governance framework, recognising that rural scams often fuelled urban financial crimes (Zhao, 2019). Nigeria's policies, by contrast, largely treat rural insecurity as peripheral. China's experience underscores the importance of embedding rural realities into national digital strategies, but it also highlights Nigeria's political economy challenge: rural areas are often ignored because they lack electoral or economic visibility. Thus, the transferability of China's model depends not on technical capacity but on Nigeria's willingness to shift its policy priorities.

Taken together, these comparative cases reveal both opportunities and limits. The overarching lesson is not that Nigeria should directly adopt the strategies of India, Kenya, Brazil, or China, but that it must design context-sensitive adaptations. For example, rather than importing mobile labs, Nigeria could develop regional forensic hubs; instead of constitutional-level fiscal decentralisation, Nigeria could establish ring-fenced rural security funds; instead of fully cloud-based forensic tools, Nigeria might begin with hybrid offline-online systems resilient to poor connectivity.

Ultimately, comparative case studies demonstrate that Nigeria's rural forensic challenges are not insurmountable but require tailored solutions grounded in its governance realities. The critical insight is that successful models abroad combined innovation with structural reforms—and unless Nigeria addresses its own governance, accountability, and security deficits, even the most advanced external models will fail to take root.

4.7 Conclusion

These case studies demonstrate that other developing countries like Nigeria suffer similar rural forensic inefficiency in the past, though still on the quest or pathway to curb the digital forensic limitations, hence, can be overcome through localized innovation, interagency collaboration, community engagement, and targeted investment. For Nigeria, integrating lessons from countries like India, Kenya, Brazil, South Africa, and the Philippines will

require adaptive policymaking, decentralized implementation, and strong partnerships between government, civil society, and the private sector.

4.8 Summary

This chapter examines how other developing countries such as India, Kenya, South-Africa, Phillipines and Brazil have addressed rural forensic challenges through policies, infrastructure investment, inter-agency collaboration, and capacity-building initiatives. These case studies reveal practical approaches that Nigeria can adapt to strengthen its own rural forensic systems. Building on these insights, chapter five engages in further critical discussion of deployment of both the digital forensic equipment and human person (Investigators) to rural communities, contextualises them within further theoretical framework and proposes recommendations tailored to Nigeria's rural realities.

5 Deployment of Digital Forensic Tools from Urban to Rural Communities

5.1 Introduction

The deployment of digital forensic tools from Nigeria's urban centres to rural communities is often framed as a logistical problem, primarily attributed to poor road networks, insecurity on highways, and inadequate transport systems. While these obstacles are significant, a more critical analysis reveals that the issue reflects deeper structural weaknesses in Nigeria's governance, security architecture, and technological adaptation. The challenge is less about physical movement of equipment and more about the state's inability to design deployment strategies that account for rural realities. At the surface level, transporting sensitive forensic tools from Abuja or Lagos to remote rural areas is hampered by insecurity like kidnappings, armed robberies, and attacks on law enforcement convoys are common along major highways [49]. However, insecurity itself is not an isolated barrier; it is evidence of state fragility and weak monopoly of violence, which directly undermines the credibility of rural forensic deployments. Moving high-value digital equipment in such contexts is not merely difficult but strategically dangerous, exposing both personnel and technology to theft or destruction.

Beyond insecurity, the digital literacy gap among rural officers poses another underexplored challenge. Even when forensic devices reach rural commands, officers often lack the training or confidence to operate them effectively. This results in under-utilisation or misuse of tools, leading to flawed investigations [50]. The problem therefore lies not only in the logistics of deployment but also in the absence of capacity-building systems that ensure sustainable use once the equipment arrives. Subsequently, comparative evidence underscores the importance of context-sensitive solutions. In Brazil, forensic investigators overcame geographical and infrastructural barriers by adopting satellite technologies, drones, and cloud-based forensic platforms, reducing dependence on physical transport (Silva & Ramos, 2019). India deployed mobile digital forensic labs in vans to rural districts, bringing services closer to remote communities (Mehta, 2020). Nigeria, however, faces unique challenges such as high insecurity makes mobile labs vulnerable to attack, while unreliable internet connectivity undermines cloud-based alternatives. These comparisons suggest that Nigeria cannot simply "copy and paste" foreign models but must adapt solutions to its security and infrastructural environment.

The consequences of weak deployment strategies are profound. Rural cybercrime investigations are often delayed, compromised, or entirely abandoned due to lack of timely access to forensic tools. This creates safe havens for criminal networks, particularly those engaged in mobile banking fraud, human trafficking, and terrorism financing. Over time, this neglect undermines not only rural security but also Nigeria's broader national and international security posture. Therefore, the challenge of deploying digital forensic tools to rural Nigeria

should not be reduced to logistical shortcomings. It must be reconceptualised as a governance and innovation issue. Nigeria requires hybrid approaches such as establishing strategically located regional forensic hubs, developing lighter and more portable forensic kits suitable for insecure terrains, and embedding secure digital reporting systems that reduce reliance on physical transport. Without such structural innovation, rural communities will remain systematically excluded from digital justice. No wonder Adeniyi & Olayiwola, 2020 in affirmation stated that the deployment of digital forensic tools from urban centres to rural communities is not only a question of technological availability but also of physical accessibility. One of the most significant barriers to this process in developing countries such as Nigeria is the state of road infrastructure. Poor road networks characterised by unpaved roads, erosion damage, seasonal flooding, and inadequate maintenance hinder the timely and efficient movement of forensic equipment, personnel, and mobile laboratories from urban hubs to rural areas. Unlike urban centres, where digital forensic laboratories are often concentrated, rural communities are geographically dispersed and accessible only through unreliable transport routes, limiting the capacity for rapid forensic response. This chapter addresses these issues by unpacking three interrelated themes: (1) poor road network and geographical mapping; (2) insecurity situation on Nigerian roads/air and safety consideration; and (3) rural dwellers alien to digital forensic knowledge. The discussion that follows underscores how these deployment challenges translate into real-world digital forensic investigative failures in rural areas.

5.2 Theme One: Poor Road Network and Geographical Mapping

In the context, Eze et al., 2019 stated that digital forensic investigation's timeliness is critical. He opined that evidence from mobile devices, computers, or digital storage media can easily be lost, tampered with, or rendered inadmissible if not collected promptly. However, when investigators must navigate poorly maintained rural roads, which are often impassable during rainy seasons, the delay in reaching crime scenes becomes a major obstacle. For example, in parts of Northern and Southern Nigeria, deteriorated federal roads have been reported to extend travel times from urban centres by several hours or even days, making it difficult to deploy forensic kits and preserve digital evidence (Eze et al., 2019). This logistical challenge undermines the credibility of investigations and often leaves rural communities underserved in terms of access to justice.

The reliance on mobile forensic laboratories or "forensic vans," which has proven effective in countries such as South Africa under the Integrated Rural Justice Project (IRJP), demonstrates how mobility is a prerequisite for rural forensic accessibility. In South Africa, well-connected road infrastructure enabled forensic-equipped vans to reach remote communities for on-site evidence capture (Louw, 2018). However, replicating such models in Nigeria has been difficult due to poor road linkages between urban forensic hubs like Lagos or Abuja and rural hinterlands. This infrastructural gap means that while urban areas may benefit from state-of-the-art forensic facilities, rural communities remain excluded.

Furthermore, poor road networks also increase operational costs for forensic agencies. Vehicles carrying sensitive forensic devices face frequent breakdowns when travelling across damaged terrain, which not only delays investigations but also risks damaging expensive equipment. According to Onwuemele (2018), the high cost of transportation in Nigeria's rural areas largely attributed to poor road infrastructure which has a direct effect on the efficiency of service delivery. In the forensic context, this translates into higher deployment costs, reduced frequency of rural forensic interventions, and a growing disparity between urban and rural justice systems. Similarly, the limited road access often compels rural investigators to rely on alternative, less secure methods of evidence transport, such as commercial motorcycles or informal couriers, which expose sensitive digital evidence to risks of tamper-

ing or contamination (Okonkwo, 2021). Such practices compromise the chain of custody, a crucial element in digital forensic admissibility in court.

On the other hand, accurate geographical mapping is an essential prerequisite for effective digital forensic deployment, particularly in rural communities where spatial precision directly impacts evidence collection and investigative timelines. In Nigeria, the absence of standardized addressing systems across many villages significantly complicates law enforcement operations. Despite the Nigerian Postal Service (NIPOST) introducing national addressing frameworks and the government's proposed Proof-of-Address system, implementation remains inconsistent, thereby undermining forensic reliability in rural contexts (NIPOST, 2025). Equally another issue is the fragmented availability of baseline geospatial datasets. While initiatives such as GRID3 have generated national settlement and infrastructure maps, coverage disparities persist, necessitating heavy reliance on local community knowledge to complement digital datasets (Sinha et al., 2021). Moreover, telecommunications coverage maps, though increasingly harmonized by the Nigerian Communications Commission (NCC), reveal large discrepancies between urban and rural areas. Rural communities often depend on 2G networks with wide cell-site radius, reducing the precision of location-based forensic techniques such as call detail record (CDR) analysis or geofencing (NCC, 2023). Additionally, crowd-sourced geospatial data, particularly OpenStreetMap, provides valuable supplementary insights into uncharted rural routes and settlements. However, its urban bias and variable accuracy raise questions of admissibility and forensic validity (Goodchild, 2019). Consequently, incomplete or unreliable geographical mapping continues to hinder the operational effectiveness of digital forensics in rural Nigeria Inadequate road networks and geographical mapping largely constitute a fundamental hindrance to the deployment of digital forensic tools from urban to rural communities. Hence, without significant infrastructural improvement, rural areas in Nigeria and similar developing countries will continue to face systemic exclusion from timely digital forensic services, thereby widening the urban–rural divide in criminal investigation and justice delivery.

5.3 Theme Two: Insecurity on the Nigerian highways and Air challenges

Insecurity on Nigeria's transport corridors and recurrent air-travel disruptions significantly hinder the timely deployment of digital forensic capabilities from urban hubs to rural communities. Firstly, highway insecurity manifested in armed robbery, banditry and mass kidnapping directly raises the risk profile, transit time and insurance costs for moving investigators, evidence and fragile instruments by road or air. Empirical and review studies document widespread highway victimisation across the federation, with the Abuja–Kaduna and North-West corridors repeatedly highlighted as hotspots (Ugwuoke, 2023). Contemporary incident data show the persistence and spatial diffusion of kidnap-for-ransom operations into peri-urban and rural catchments, degrading the reliability of inter-city travel and logistics (Reuters, 2024; Global Initiative, 2024; SBM Intelligence, 2024). Forensic fieldwork that depends on rapid first response imaging volatile devices, seizing network artefacts, or preserving chain-of-custody becomes delayed or cancelled as teams avoid night travel, reroute to longer "safer" roads, or require armed convoying, each adding hours to evidence acquisition windows. These constraints are not merely anecdotal, however, sector analyses of interstate transport in North-Central Nigeria identify operational slowdowns, route abandonments, and higher transport tariffs linked to banditry and kidnapping (Ohida, 2022; FUTA Journal Study, 2025). The cumulative effect is a form of "infrastructural friction" that undermines rural forensic readiness including mobile labs and write-blockers arrive late, batteries discharge before use, and suspects exploit lag times to wipe devices or move SIMs. The 2022 Abuja–Kaduna rail attack which suspended a critical inter-city alternative for eight months illustrates how shocks to a single corridor cascade into wider mobility deficits for technical teams who would otherwise bypass unsafe highways (Al Jazeera, 2022; Wikipedia

summary, 2025).

5.4 Theme Two: Insecurity on the Nigerian highways and Air challenges

In the same situation, Air mobility often proposed to leapfrog insecure roads faces its own structural and seasonal limitations. Although Nigeria lists roughly 31 airports and numerous airstrips/heliports, passenger activity is highly concentrated, with a small number of airports handling most of the traffic (NCAA, n.d.; The Guardian, 2024). For many rural destinations there is no scheduled service, forcing indirect routes and last-mile road transfers that reintroduce security exposure. This means that reliability is further undermined by dry season harmattan hazard, when degraded visibility triggers widespread delays and cancellations; aviation regulators routinely issue seasonal cautions and warn operators to expect disruptions (NCAA, 2019; AviationMetric, 2023). Recent operational snapshots underscore the scale of irregularity in September to October 2024, roughly half of Nigerian domestic flights were delayed and nearly 200 cancelled, with regulators linking recurrent disruptions to weather and operational factors (The Sun, 2025; Peoples Gazette, 2024). By implication, forensic deployments that depend on assured arrival within narrow evidentiary windows are therefore jeopardised, while budget lines must absorb rebooking, accommodation and standby costs.

5.5 Theme Two: Insecurity on the Nigerian highways and Air challenges

The interaction of highway insecurity and air-travel fragility produces a reliability gap that disproportionately affects rural digital investigations. Where urban labs can coordinate within dense, policed corridors, rural cases suffer elongated response times, weakened chain-of-custody, and increased investigator risk. Policy responses visible in the transport and security literature hardening key corridors, restoring safe rail alternatives, and improving seasonal aviation operations are thus not merely mobility goals; they are prerequisites for equitable forensic access outside Nigeria's cities (Ugwuoke, 2023; Reuters, 2024; NCAA, n.d.).

5.6 Theme Three: Rural Dwellers' Knowledge Alien to Digital Forensic Investigation and Practice

A recurring theme in scholarship on the "last mile" of criminal investigation is the mismatch between forensic practice assumptions and rural realities. Digital forensic workflows and tools are typically designed with urban, well-resourced contexts in mind; when these technologies are moved into rural communities, the sociocultural and knowledge gaps of local populations frequently become a primary barrier to effective deployment (Dijk 2005). This section synthesises literature on how rural dwellers' limited familiarity with digital technology, differing conceptions of evidence and privacy, and local knowledge systems impede digital forensic investigation and the uptake of forensic devices.

i) Digital Literacy Gap

First, the digital literacy gap matters because forensic processes assume basic user knowledge about devices and data. Digital forensics depends on structured interactions with devices (preserving chains of custody, identifying likely evidence locations, and understanding device usage patterns). Yet rural populations often have lower rates of formal digital literacy and less exposure to complex device ecosystems, leading to difficulties in explaining device histories, relevant accounts, or passwords to investigators (UNESCO, 2018). The consequence is both practical lost time during triage, increased risk of contamination and epistemic, since investigators may misinterpret benign local digital practices as suspicious

(Casey, 2011). For example, in many rural settings like Amede, a single mobile phone may be shared among extended family members; without awareness of this practice, an examiner may attribute multiple identities to one user or overlook communal usage as relevant context (Dijk, 2005). Similarly, local cultural frameworks for evidence and testimony differ from forensic presumptions. Digital forensics is rooted in models of individual ownership and discrete, time-stamped artefacts; many rural communities operate on collective ownership, oral records, and social rather than technical proofs of events. Such divergences complicate both evidence collection and admissibility. Studies on community justice initiatives show that elders' testimony and social reconciliations are often prioritised over documentary or digital artefacts, thus investigators may find limited cooperation when asking for device seizure or long-term retention (Eze et al., 2016). He added that where investigators do not adapt to these cultural grammars, they may provoke distrust, resistance, or strategic concealment of devices.

ii) Mistrust and Misconception about Technology

According to Oyedepo 2013 stated that this can lead to non-cooperation or tampering. Furthermore, in some rural communities, devices are associated with surveillance, witchcraft, or external authority requests to hand over phones or permits for forensic imaging may trigger resistance or intentional destruction of potential evidence (UNESCO, 2018). The literature on adoption of technology emphasises that perceived risk and lack of transparency reduce willingness to participate in technical processes (Dijk, 2005). As a result, mobile field units and portable forensic kits face not only logistic challenges but also socio-cultural opposition that reduces their effectiveness. On the other hand, linguistic and procedural communication problems are well dealt with. Effective forensic triage requires clear explanation of procedures and consent language barriers and low technical vocabulary among rural dwellers make informed consent and accurate interviews difficult (Casey, 2011). The absence of locally adapted informed-consent materials and the scarcity of culturally competent forensic liaisons means that critical steps (e.g., documenting chain of custody or ensuring device password disclosure under lawful conditions) are frequently undermined.

Furthermore, the literature points to promising mitigations, community engagement, co-design, and capacity-building. Rather than imposing urban-centric workflows, investigators who invest in community sensitisation, translate procedures into local languages, and collaborate with trusted local authorities obtain higher cooperation and more reliable evidence collection (Eze et al., 2016). Training local paralegals or "forensic intermediaries" who understand both local norms and basic digital handling has been proposed as a scalable bridge (UNESCO, 2018). Examples from analogous fields mobile health deployments and rural election monitoring show that participatory design and visible safeguards against misuse dramatically increase acceptance of technical interventions.

In summary, rural dwellers' relative unfamiliarity with digital devices, divergent norms about ownership and evidence, mistrust of external actors, and communication gaps create a distinct barrier to deploying digital forensic devices in rural communities. The literature argues that technical solutions alone (portable kits, ruggedised hardware) will fall short without parallel investments in culturally informed outreach, local capacity building, and adaptation of forensic methods to communal and oral knowledge systems (Casey, 2011; Van Dijk, 2005; World Bank, 2016; UNESCO, 2018). Addressing the knowledge alienation of rural populations is therefore a necessary precondition for meaningful and ethical forensic deployment.

5.7 Challenges in Rural Deployment and Initiatives to Enhance Rural Forensic Capabilities

Recognizing these challenges, initiatives to bridge the digital forensic gap between urban and rural communities as well as possible deployment, the Scalable Rural Digital Forensics Initiative (RDFI), funded by the U.S. Department of Justice, aims to support rural law enforcement agencies by providing training, resources, and access to digital forensic technologies is a take home lesson for Nigeria. The program includes establishing digital forensics laboratories, integrating high-quality digital content creation studios, and developing digital/social media delivery mechanisms to reach law enforcement in rural communities. Similarly, the University of Southern Mississippi's Rural Digital Forensics Initiative 2024 focuses on developing a training lab solution for digital forensics applicable to rural communities across the United States. This initiative includes establishing a working digital forensics laboratory and digital content production studio on the university campus, which are used to create training content for law enforcement to better understand digital forensics processes and capabilities.

5.8 Examples of Successful Deployment in the United Kingdom

In the United Kingdom, the National Police Chiefs' Council's research on Digital Forensic Science Strategy 2020 underscores the importance of digital forensics in modern policing. The strategy aims to expand digital forensic capabilities beyond traditional forensic units, enabling frontline staff to conduct digital forensic work. This approach ensures that digital forensics are integrated into the investigative process from crime scene to courtroom, enhancing the efficiency and effectiveness of investigations. Furthermore, advancements in mobile digital forensic kits have enabled rural law enforcement agencies to conduct preliminary analyses on-site. These portable tool kits, according to research from the University of Hawaii Maui College, allow investigators to perform live analysis of digital devices, such as smartphones and tablets, at the crime scene, reducing the need to transport devices to distant laboratories and expediting the investigative process.

5.9 Conclusion

The deployment of digital forensic devices from urban to rural communities necessitates addressing road network disparities, providing specialized security coverage, and implementing rural forensic knowledge solutions. By investing in these areas, deployment of these devices and rural law enforcement agencies can enhance their investigative capabilities, ensuring that digital evidence is effectively utilized to solve crimes and uphold justice.

5.10 Summary

This chapter synthesises findings from Nigeria and lessons from other contexts to critically assess the systemic nature of the country's forensic challenges. It demonstrates how infrastructural neglect, institutional weakness, and human resource deficits interlock to perpetuate rural forensic exclusion. Guided by the theoretical framework, the chapter proposes actionable recommendations such as investment in rural ICT infrastructure, capacity-building for law enforcement, policy harmonisation, and community-based forensic awareness programmes. To consolidate the argument, the study concludes by summarising its contributions and pointing to avenues for further research, as presented in chapter six.

6 Discussion, Conclusion and Recommendations

6.1 Discussion of Findings

The findings of this study confirm that digital forensic investigation in Nigeria's rural communities is fraught with challenges that severely undermine its effectiveness. The study

revealed four major limitations: lack of infrastructure, institutional fragmentation, insufficient capacity, and weak policy implementation. These findings are consistent with prior literature which highlights the urban-rural divide in law enforcement capabilities (Ayo, 2021; Ogunbodede, 2022).

Infrastructural deficits, such as unreliable electricity and lack of forensic labs, mirror the conditions observed in other developing nations where centralized forensic systems neglect rural peripheries. The lack of trained personnel further compounds the issue, as digital crimes increasingly require technical knowledge that rural officers often lack. These conditions foster a justice gap that allows cybercrimes in rural areas to go unresolved or unreported. Hence, the perpetrators of criminal activities in cities are taking advantage of the porous nature of rural counterpart for hideout, kidnapped hostage and terrorist den.

6.2 Chapter Two

This chapter has highlighted the critical policy and legal weaknesses that obstruct the implementation of digital forensics practice in Nigeria's rural regions. The analysis reveals that rather than serving as enablers, current policy and legal structures often act as barriers to the practice of digital forensics in low-resource environments. The fragmentation of forensic governance across agencies that causes confusion over roles and responsibilities is not left out, particularly in rural cases involving digital crime. This disjointed structure fails to provide rural law enforcement with clear escalation protocols or operational mandates thereby creating more Inter-agency rivalries and lack of collaboration mechanisms resulting to digital evidence often get lost in bureaucratic limbo.

The Nigeria's legal regime for digital evidence underdevelopment, possess a great concern in national discourse. This includes, while electronic evidence is technically admissible in court, the procedural frameworks for collecting and authenticating such evidence are inadequate. In rural areas, this legal vagueness is exacerbated by a lack of legal training and infrastructural support. The outcome therefore is often the dismissal of cases for lack of evidence, regardless of digital indicators available. Furthermore, Nigeria's national digital and cybersecurity policies do not prioritize rural inclusion. The absence of rural-specific strategies means that forensic justice remains a distant goal for many underserved communities. Without grassroots consultation and adaptive policymaking, national strategies risk reinforcing rather than resolving digital inequality.

The implications of these findings are largely profound and if Nigeria aims to build a credible digital forensic framework, it must embed rural access and participation at the heart of legal and policy reform. Suggested interventions include the creation of a centralized national forensic coordination body, amendment of existing laws to incorporate detailed forensic protocols, and the integration of rural-focused initiatives in national cybersecurity plans, drawing a lesson from developed countries like Japan and China's deliberate integration of rural-specific needs into broader development strategies. Until such structural reforms are made, digital forensic practice in rural Nigeria will remain constrained not just by technology gaps, but by the very laws and policies that are meant to empower it. The findings from this literature review offer critical insights into the structural and operational limitations confronting digital forensic investigations in Nigeria's rural communities. While the country's legal and institutional frameworks for digital justice are maturing, a deep rural-urban divide continues to undermine equitable access to forensic technologies and justice mechanisms.

6.3 Chapter Three

The findings in this chapter reveal a deeply rooted infrastructural divide that undermines the viability of digital forensic investigations in Nigeria's rural communities. Unlike urban centres equipped with digital laboratories and skilled personnel, rural areas are systematically marginalized in terms of technological deployment and investigative support. First, the absence of nearby forensic laboratories and tools forces rural officers to rely on inefficient manual processes or transport evidence over long distances, increasing the risk of contamination and legal inadmissibility. The centralization of forensic facilities reflects broader inequalities in public resource allocation, which disproportionately affects local justice systems.

Second, digital connectivity and electricity as foundational components of modern forensic work remain unreliable or non-existent in most rural regions. Without stable internet and power, digital evidence cannot be securely stored, transmitted, or processed. This not only delays investigations but also weakens Nigeria's broader cybersecurity posture, especially in regions vulnerable to localised cybercrime or terrorism.

Third, the lack of technical training and organizational support for rural law enforcement exacerbates these infrastructural gaps. Even when digital evidence is accessible, officers often lack the skills to manage it. This problem is intensified by the absence of institutionalized knowledge-sharing networks, mobile forensic teams, or community-based tech collaborations. The implications of these findings are significant. In rural Nigeria, where digital crimes such as mobile fraud, terrorism, kidnapped-victim-hostage-camp, election tampering, or online sexual exploitation are on the rise, the inability to investigate effectively allows perpetrators to act with impunity. The current infrastructural landscape effectively excludes rural communities from the benefits of forensic justice, widening the rural-urban justice divide and undermining national security and legal equity. Addressing these challenges will require a multi-layered approach. Infrastructure development must include not just roads and electricity but digital connectivity and forensic capacity. Federal and state governments should decentralize forensic laboratories and invest in mobile forensic units that can serve remote areas. Moreover, partnerships with private sector forensic firms, universities, and international donors can bridge training gaps and supply basic forensic kits to rural police stations. Therefore, this chapter thus concludes that infrastructure is not a peripheral issue but a central pillar in the effective administration of digital forensic justice. Hence, without addressing the infrastructural limitations identified, any effort to strengthen forensic capacity in Nigeria's rural communities will remain incomplete and unsustainable.

6.4 Chapter Four

These case studies highlight several key lessons for Nigeria:

1. 1. Decentralization works: India and Brazil demonstrate that creating regional or mobile forensic hubs can improve rural access, reduce delays, and protect evidence integrity.

2. 2. Training must be inclusive: Kenya and South Africa show that rural officers can become effective digital investigators if provided with localized, language-sensitive training.

3. 3. Technology partnerships are critical: Kenya and the Philippines effectively leverage partnerships with telecom firms, universities, and NGOs to bridge technical gaps.

4. 4. Community engagement builds trust: South Africa's model emphasizes community empowerment, which fosters cooperation and crime reporting in rural areas.

5. 5. Legal flexibility enhances reach: The Philippines' adaptive frameworks ensure local law enforcement units can respond without waiting for central approvals.

6. For Nigeria, these experiences provide a roadmap, this includes establishing mobile forensic labs, integrating training into rural police curricula, forming ICT-based partnerships, and empowering communities through education can help transform rural digital forensics. Importantly, any solution must be context-specific, rooted in Nigeria's socio-political realities, and driven by long-term investments in rural justice systems.

6.5 Chapter Five

Deployment of digital forensic tools from Nigeria's urban hubs to rural communities is encumbered by intertwined infrastructural, security, and sociotechnical barriers. First, logistics chains are brittle because road conditions are poor across vast stretches of the network, inflating travel time, risk of equipment damage, and costs for mobile labs and incident response teams; recent assessments estimate a very high share of roads in poor condition, undermining service delivery to rural populations (BusinessDay, 2025). Second, pervasive insecurity on intercity corridors including banditry and kidnapping along highways creates substantial risks for evidence couriers and field investigators, often necessitating armed escorts, route diversions, or flight alternatives that are themselves occasionally affected by broader security dynamics (Reuters, 2024; The Guardian, 2024; UNIDIR, 2024). These constraints complicate chain-of-custody integrity, timeliness of device triage, and continuity of operations for time-sensitive cybercrime inquiries.

Third, a pronounced rural–urban digital literacy gap limits local first responders' capacity to preserve volatile digital evidence (e.g., isolating devices, avoiding data spoliation) and constrains community cooperation in technology-mediated investigations (Olanrewaju, 2021; Okocha, 2023/2025). Where literacy is low, community members may inadvertently wipe data or resist consensual data collection. Finally, technical mistrust rooted in wider institutional distrust and debates about surveillance and data rights reduces willingness to engage with police digital tools (e.g., mobile extraction kits, digital IDs), thereby impeding consent-based acquisition and tip-line uptake (Okunoye, 2022; Tiwa, 2024).

Targeted mitigation requires (i) hardened logistics (shock-proofed kits, redundant power, satellite backhaul) and secure transport protocols tailored to high-risk corridors; (ii) regional staging nodes to shorten last-mile travel; (iii) rural digital-evidence awareness training for health workers, teachers, and traditional leaders as "first receivers" of incidents; and (iv) community-embedded accountability mechanisms (transparent audit trails, civilian observers, and clear consent artefacts) to counter mistrust and enhance legitimacy of digital forensic practices in rural Nigeria. The deployment of digital forensic devices from urban to rural communities necessitates addressing road network disparities, providing specialized security coverage, and implementing rural forensic knowledge solutions. By investing in these areas, deployment of these devices and rural law enforcement agencies can enhance their investigative capabilities, ensuring that digital evidence is effectively utilized to solve crimes and uphold justice.

6.6 Implications of the Study

The implications of this study are significant for policy, law enforcement, and academic. For policymakers, the findings underscore the need to decentralize digital forensic services and embed them within rural police divisions. For law enforcement agencies, the results highlight the urgency of investing in rural officer training and equipment. Academically, the study offers a basis for further research on rural digital justice systems and forensic inequality.

6.7 Recommendations

Based on the critical findings, the following recommendations are therefore proposed to bridge the gap between urban and rural Nigeria in her fight against insecurity in the country.

i. Infrastructure Investment: Nigerian government and private sector partnerships should prioritize infrastructure in rural communities, particularly road network, power supply, internet connectivity and digital equipment in police stations and other formations of a similar statutory law enforcement agency like the DSS and EFCC.

ii. Decentralization of Forensic Services: The government in her constitutional mandates establish forensic laboratories and mobile forensic units in rural regions to reduce dependency on urban centres.

iii. Capacity Building: Introduce mandatory digital forensic training in law enforcement police academies, judiciary colleges and offer continuous education for rural officers.

iv. Legal and Policy Reform: Adapt the Cybercrimes Act (2015) and other relevant frameworks to address rural realities, including legal aid for rural communities.

v. Community Engagement: Develop public awareness campaigns to educate rural populations on digital evidence and cybercrime reporting.

vi. Monitoring and Evaluation: Establish a system to periodically assess digital forensic capacity and gaps in rural regions.

6.8 Suggestions for Further Research

Digital forensic investigation in Nigeria's rural communities is an underexplored area of scholarship, and this study has highlighted numerous gaps in infrastructure, policy, and practice that constrain effective operations. While these findings contribute to ongoing debates about forensic science in developing contexts, they also open avenues for more nuanced inquiries. This section outlines key suggestions for further research that can help strengthen both theoretical understanding and practical implementation of digital forensics in rural Nigeria.

i. Comparative Studies Across Developing Countries
One important area for future inquiry lies in comparative research. Examining how other developing countries particularly those in Sub-Saharan Africa, South Asia, and Latin America have approached the rural–urban digital divide could provide valuable lessons for Nigeria. For instance, Kenya's mobile-driven innovations in digital policing and India's community-based forensic training models demonstrate potential pathways for countries facing infrastructural limitations [51]. Comparative studies would not only highlight transferable best practices but also identify culturally specific challenges that shape digital forensic adoption.

ii. Integration of Emerging Technologies
Another promising direction involves exploring how emerging technologies such as artificial intelligence, blockchain, machine learning, and cloud-based forensics could be adapted for rural environments. While these tools are often deployed in technologically advanced contexts, they may hold potential for resource-limited settings if tailored appropriately (Aliyu, 2022). Future research should assess the feasibility, cost-effectiveness, and ethical implications of deploying lightweight, decentralized technologies to support rural digital investigations in Nigeria.

iii. Policy and Legal Frameworks
Although Nigeria has enacted laws such as the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, these frameworks have been critiqued for being urban-centric and poorly enforced in rural areas (Adebayo & Ojo, 2021). Further research is needed to interrogate the adaptability of existing policies to rural realities. Empirical studies could focus on enforcement gaps, jurisdictional issues in rural settings, and the role of local governance in bridging forensic capacity deficits.

iv. Community-Based Forensic Models
Another underexplored area is the development of grassroots-driven forensic models. Research could examine how local law enforcement officers, community leaders, and even civil society organizations might be trained in basic digital evidence preservation techniques. Such work would assess whether decentralizing aspects of forensic investigation can reduce dependence on urban centers and foster trust between communities and investigators [52].

v. Cost–Benefit Analysis of Infrastructure Investment
Empirical economic research could analyze the financial implications of expanding forensic infrastructure into rural regions. By conducting cost–benefit analyses, scholars can provide evidence-based arguments for policy advocacy, demonstrating how investment in forensic facilities might reduce crime, enhance security, and promote rural socio-economic stability (Eze, 2019). Such studies would also explore whether mobile forensic laboratories or satellite-based systems offer more sustainable alternatives to permanent infrastructure.

vi. Inter-Agency Collaboration in Rural Settings
Fragmentation among Nigerian security agencies has long been identified as a barrier to effective forensic practice (Oluwatobi, 2021). Further research should investigate models of inter-agency collaboration that are specifically tailored to rural environments, where resources are limited and coordination is essential. Case studies of successful collaborative frameworks in other jurisdictions could inform practical recommendations for Nigeria.

vii. Digital Literacy and Human Capacity Development
Future studies should focus on the role of digital literacy in rural communities. Limited awareness of forensic processes can hinder cooperation with investigators, create mistrust, and compromise the integrity of evidence collection. Research into community education programs, law enforcement training initiatives, and the integration of digital literacy into rural school curricula could offer long-term solutions to this challenge [53].

viii. Socio-Cultural Barriers to Digital Forensics
Beyond technical constraints, social and cultural dynamics warrant deeper exploration. For instance, mistrust of technology, fear of surveillance, and local beliefs about evidence handling may obstruct forensic processes. Ethnographic and sociological research can provide insights into these barriers, ensuring that forensic strategies are not only technologically sound but also culturally sensitive (Chukwu, 2021).

ix. Case Study-Oriented Research
Given the diversity of Nigeria's rural communities, localized case studies could generate rich insights into context-specific challenges. Detailed examinations of digital forensic investigations in particular states or local government areas would highlight variations in infrastructure, community cooperation, and legal enforcement. Such micro-level studies could feed into broader national strategies while ensuring that policy solutions are grounded in real-world conditions.

x. Infrastructure and Connectivity Alternatives

Finally, research should examine alternative models of rural connectivity. Renewable energy solutions, mobile forensic units, and satellite-based internet systems present potential ways of overcoming infrastructural deficits. Studies could explore the technical feasibility, sustainability, and social acceptability of such innovations, thereby offering pathways for extending forensic capacity to underserved regions (Nwosu, 2022). Therefore, the above suggestions point to the need for multidisciplinary approaches that combine insights from law, criminology, information technology, economics, and sociology. By pursuing these avenues of research, scholars and policymakers can deepen understanding of Nigeria's rural forensic landscape and design more inclusive, context-sensitive solutions. Ultimately, bridging the forensic divide between rural and urban Nigeria will not only enhance crime investigation but also strengthen national security and justice delivery.

6.9 Conclusion

This study has explored the critical limitations facing digital forensic investigations in Nigeria's rural communities. Through literature-based study methods, it revealed deep-seated infrastructural, institutional, and legal challenges that hinder effective cybercrime prosecution outside urban centres. The findings call for a multi-stakeholder approach involving government, law enforcement, academia, and communities to bridge this gap. As digital crimes become more pervasive, it is imperative that no region is left behind. By strengthening forensic capacity in rural areas, Nigeria can move towards a more inclusive, effective, investigative and justice system that upholds digital accountability and equity across all demographics.

6.10 Summary

The final chapter revisits the central research problem and demonstrates how the study has addressed it by identifying Nigeria's rural digital forensic limitations, analysing them through a theoretical lens, and drawing comparative lessons from other countries. It highlights the study's academic contribution to digital forensic literature, practical recommendations for policymakers, and limitations that open pathways for future research. In doing so, the conclusion ties the analysis back to the research aim introduced in chapter one, thereby closing the loop of the dissertation.

Acknowledgments

I am deeply grateful to God Almighty for the strength, wisdom, and guidance throughout the course of this research and especially his ever-sufficient grace to make the programme a huge success.

My sincere appreciation to my supervisor, Dr. John Akerele, whose unwavering support, insightful guidance, and constructive feedback have been invaluable in shaping this dissertation. Indeed, your encouragement and mentorship have not only enhanced the quality of this research but also my academic growth. I also wish to extend my gratitude to the faculty and staff of University of Portsmouth, Humanities and Social Sciences, and school of Criminology and Criminal Justice for providing the academic environment and resources necessary for this study. Special thanks to my lecturers, especially the faculty coordinator, Dr. Maggie Bower, the CLTs, Dr. Laura Haggar and Alejandra De La Fuente, my mentors, particularly Dr. Uchenna Ogenyi and my course mates like Natalie Lejeune, Shameel Sakheer, Obianuju Felicia Okoli, Asan, Dammy, Mariam, Amelia and Ellie whose contributions, discussions, and encouragement enriched my knowledge.

To my Angel turned wife, Mrs. Chinenye Jessica Odo (RN), I owe a debt of gratitude for your exceptional love, understanding, and constant support. To my parents, Mr & Mrs Louis and Comfort Odo, my siblings especially Oluchi Esther Olinya and her husband, Chidi Samuel Olinya, your prayers and encouragement have kept me motivated, during challenging times

and joyful moments.
Lastly, I salute all the authors, scholars, and practitioners numerous to mention here, whose works were consulted during this dissertation. Their insights are quite impactful, hence provided the foundation upon which this study was built. And to everyone who contributed in one way or another to the success of this research, I say thank you and remain ever blessed.

References

[1] Ogunleye, T., & Adedayo, F. (2022). Challenges in Evidence Collection and Preservation in Nigeria's Rural Law Enforcement. Nigerian Journal of Criminology and Security Studies, 8(2), 101–118.

[2] Chinwendu, O., & Eze, S. (2021). Digital Forensics and Cybercrime Investigation in Nigeria: Challenges and Prospects. Journal of Information Security, 12(3), 45–60.

[3] Ishaq, A., & Yusuf, M. (2020). The State of Digital Forensic Readiness in Nigeria: An Evaluation of Infrastructure and Capacity. African Journal of Computing & ICT, 13(2), 22–34.

[4] Nwokedi, C., & Okeke, P. (2019). Cybercrime and Digital Forensics in Rural Nigeria: Bridging the Capacity Gap. International Journal of Cybersecurity Studies, 5(1), 15–28.

[5] Okoro, B., & Adebayo, K. (2020). Digital Literacy and Cybercrime Reporting in Rural Nigeria. Journal of Digital Society, 6(1), 33–48.

[6] Casey, E. (2019). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (4th ed.). Academic Press.

[7] Osho, G., & Onoja, A. (2021). Comparative Perspectives on Cybercrime Regulation in Africa. Journal of Law and Technology in Africa, 7(1), 34–50.

[8] Adebayo, F. (2020). Challenges of Digital Forensics in Developing Economies: The Nigerian Perspective. Journal of Information Security Research, 11(2), 45–58.

[9] United Nations Office on Drugs and Crime (UNODC). (2022). Global Programme on Cybercrime: Strengthening Digital Evidence and Forensic Capacity in Developing Countries. UNODC Publications.

[10] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319–340.

[11] Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. Decision Sciences, 39(2), 273–315.

[12] Meyer, J. W., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology, 83(2), 340–363.

[13] DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. American Sociological Review, 48(2), 147–160.

[14] Oyelude, A. A. (2020). Digital Forensics and the Nigerian Legal System: Challenges and Prospects. Library Philosophy and Practice, 1–12.

[15] Ajayi, O. (2021). ICT Infrastructure and Digital Forensic Capacity in Nigeria's Rural Communities. Nigerian Journal of Information Technology, 15(1), 33–50.

[16] Nnodim, P., & Eze, K. (2020). Urban-Biased Development and the Digital Divide in Nigeria. Nigerian Journal of Development Studies, 12(4), 45–63.

[17] Mehta, R. (2019). Bharatnet and Rural Cybercrime Prevention in India. Journal of Digital Governance, 5(1), 54–72.

[18] Silva, R., & Ramos, P. (2019). Satellite and Drone-Assisted Digital Forensics in Brazil. International Journal of Digital Crime, 7(2), 33–50.

[19] Economic and Financial Crimes Commission (EFCC). (2019). Annual Report.

[20] Nigeria Police Force (NPF). (2021). Annual Report / Forensic Operations Briefs.

[21] Department of State Services (DSS). Official Website (Accessed Aug. 21, 2025).

[22] Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (Nigeria).

[23] Evidence Act, 2011 (Nigeria), Section 84.

[24] Office of the National Security Adviser (ONSA). (2021). National Cybersecurity Policy and Strategy.

[25] Central Bank of Nigeria. (2022). Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions.

[26] Nigeria Data Protection Act, 2023.

[27] Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Including 2024 Amendment Overview).

[28] Okeshola, F., & Adeta, A. (2020). The Challenges of Cybercrime Investigation in Nigeria. Journal of Cyber Criminology, 3(1), 44–59.

[29] Mutua, F. (2021). Decentralised Funding and Rural Digital Forensic Capacity in Kenya. African Security Review, 14(1), 33–52.

[30] Chukwuma, P. (2022). Funding Disparities and Cybercrime Vulnerability in Rural Nigeria. Nigerian Journal of Cybersecurity Policy, 3(1), 21–39.

[31] Adebayo, A., & Ojo, E. (2021). Digital Policing and Forensic Gaps in Nigeria. Journal of African Security Studies, 10(2), 55–70.

[32] Akinola, A. (2019). Forensic Science and Criminal Justice in Nigeria. African Journal of Criminology, 5(1), 89–104.

[33] Aghedo, I., & Osumah, O. (2012). The Police and Crime Control in Nigeria. International Journal of Police Science & Management, 14(1), 23–34.

[34] Ndukwe, C. (2021). Evidence Handling Challenges in Nigeria's Rural Policing. Nigerian Journal of Criminology, 9(2), 101–118.

[35] Mwangi, P. (2018). Rural Justice and Forensic Limitations in Kenya. East African Law Review, 12(3), 77–95.

[36] Adebayo, T. (2021). Rural Policing and Digital Evidence Handling in Nigeria. African Journal of Law Enforcement, 9(2), 78–95.

[37] Adebayo, T., & Olatunji, S. (2020). Inter-Agency Coordination and Digital Forensic Practice in Nigeria. Journal of Security Studies, 12(3), 45–62.

[38] Zhao, L. (2019). Integrating Rural Cybercrime Prevention into National Policy: The Chinese Experience. Asian Journal of Security Studies, 4(3), 77–95.

[39] Okoro, V. (2021). Retention Challenges of Forensic Officers in Nigeria's Rural Commands. International Journal of Policing Studies, 5(2), 88–105.

[40] Eze, P. (2019). Economic Implications of Security Infrastructure in Rural Nigeria. Journal of Development Policy Research, 8(2), 77–92.

[41] Oluwatobi, K. (2021). Inter-Agency Collaboration and Security Governance in Nigeria. Security Studies Review, 11(3), 88–104.

[42] Okonkwo, I. (2020). Rural Law Enforcement Morale and Professionalism in Nigeria. Journal of African Policing, 9(1), 15–34.

[43] Okeshola, T., & Adeta, K. (2019). Resource Allocation Disparities and Forensic Practice in Nigeria. Journal of Nigerian Security Studies, 11(3), 56–73.

[44] Ogunleye, A., & Adekunle, O. (2020). Training Deficits and Skill Drain in Rural Nigerian Law Enforcement. Nigerian Journal of Criminal Justice, 7(3), 22–39.

[45] Mabena, L. (2018). University Partnerships and Digital Forensic Training in South Africa. African Journal of Criminal Justice, 6(2), 77–94.

[46] Mehta, R. (2020). Mobile Digital Forensic Laboratories in India. International Journal of Forensic Science, 8(3), 45–61.

[47] Singh, R. (2020). Digital Forensics in Rural India: Challenges and Innovations. Journal of South Asian Security Studies, 5(1), 14–29.

[48] Nwosu, L. (2022). Renewable Energy and Digital Connectivity in Rural Africa. African Journal of Technology and Development, 9(1), 25–41.

[49] Owolabi, B. (2020). Deployment of Digital Forensic Tools in Nigeria: Logistical and Security Constraints. African Journal of Cybersecurity, 6(1), 40–57.

[50] Chukwu, J. (2021). Socio-Cultural Barriers to Technology Adoption in Rural Nigeria. African Journal of Social Inquiry, 12(4), 211–230.

[51] Osho, G., & Onoja, A. (2021). Digital Divide and Law Enforcement in Nigeria: Implications for Cybercrime Investigation. African Journal of Criminology and Justice Studies, 14(1), 112–129.

[52] Okafor, B. (2020). Grassroots Policing and Forensic Evidence Handling in Nigeria. Nigerian Journal of Criminology, 5(2), 120–139.

[53] Abubakar, I. (2020). Digital Literacy and Rural Security Awareness in Nigeria. Journal of Community Informatics, 16(3), 45–60.