International Journal of Innovative Information Systems & Technology Research 13(4):322-338, Oct-Dec, 2025

 www.seahipublications.org ISSN: 2467-8562

doi:10.5281/zenodo.17837021

Evaluating Law Enforcement Capabilities in Digital Forensics and Cyber Incident Management in Nigeria

Vincent Ishaya, Prof. Monday O. Adenomon, Dr. Steven I. Bassey, Prof. Gilbert I. O. Aimufua

Center for Cyberspace Studies,

Nasarawa State University, Keffi, Nigeria

ABSTRACT

This study evaluated the performance of Nigerian law enforcement agencies in digital forensic investigations and cyber incident management, focusing on the Nigeria Police Force (NPF) Cybercrime Unit, the Economic and Financial Crimes Commission (EFCC), the Department of State Services (DSS), and the National Information Technology Development Agency (NITDA). Using a mixed-methods approach, data were collected from 100 purposively selected respondents through surveys and semi-structured interviews, supplemented by analysis of institutional reports and case records. Findings reveal significant capacity gaps: only 62% of personnel have received formal digital forensics training, 75% of respondents rated current investigative performance as fair or poor, and 64% described inter-agency collaboration as ineffective. Major challenges include inadequate forensic tools and laboratories, insufficient specialized training, resource constraints, legal ambiguities in digital evidence admissibility, and fragmented coordination among agencies. Statistical analysis (chi-square and t-tests) confirmed that formal training and resource availability significantly influence investigative outcomes ($p < 0.05$). The study concludes that, despite legislative progress such as the Cybercrimes Act 2015, systemic deficiencies continue to undermine Nigeria's ability to effectively investigate and prosecute cybercrime. To address these gaps, the research proposes the Integrated Capacity and Collaboration Model (ICCM) a practical, multi-phase framework that emphasizes structured training, infrastructure development, establishment of a Joint Cybercrime Response Taskforce, legal reform, and sustained public-private-academic partnerships. The findings and proposed ICCM framework offer actionable recommendations for policymakers, law enforcement leadership, and cybersecurity stakeholders to strengthen Nigeria's digital forensic capabilities and enhance national resilience against evolving cyber threats.

Keywords: digital forensics, cyber incident management, law enforcement, cybercrime, Nigeria, capacity building, inter-agency collaboration, ICCM framework

INTRODUCTION

In today's digital world, the internet and modern technologies have brought about enormous benefits from easier communication to online banking, e-governance, and smart systems. However, this rapid digital growth has also created new risks, especially in the form of cybercrime (Akyazi et al., 2021). In Nigeria, as more people and organizations move their activities online, cyber threats have become more common and, in many cases, more damaging. Attacks such as email scams, identity theft, ransomware, and unauthorized data access are just a few examples of the digital threats facing both public and private sectors across the country (Vasanthi et al., 2021).

As cybercrime becomes more complex, there's a growing need for law enforcement agencies to keep up. One of the key areas in this fight is digital forensics, the process of investigating digital devices to uncover evidence of crimes (Sibe & Muller, 2022). Alongside this is cyber incident management, which involves responding quickly and effectively to cyber-attacks in order to reduce damage and recover operations. Together, these two areas are critical in identifying cybercriminals, collecting evidence that can stand up in court, and restoring trust in digital systems (Obidimma & Ishiguzo, 2023). Despite the importance of digital forensic investigations and proper cyber incident handling, many law enforcement agencies in Nigeria face serious limitations. These include a lack of specialized personnel, outdated or inadequate forensic tools, limited access to training, and weak coordination between agencies (Obamanu, 2018). In some cases, the legal processes for handling digital evidence are unclear or not properly enforced, making it difficult to successfully prosecute cybercrime cases. While organizations like the Nigerian Police Force, EFCC, and NITDA have taken steps to address cybercrime, their efforts are often limited by resource and structural challenges.

With cyber threats on the rise and becoming more complex, it is important to take a closer look at how well-equipped Nigerian law enforcement agencies are to deal with these issues. This includes understanding what tools and skills they currently have, what challenges they face, and how prepared they are to respond to different kinds of cyber incidents. A thorough evaluation of these capabilities will not only help identify the gaps but also provide useful direction for improving training, policy, infrastructure, and overall readiness (Ogundele et al., 2023). This study sets out to examine the state of digital forensic investigation and cyber incident management within Nigeria's law enforcement framework. By doing so, it aims to contribute to national and regional discussions on cybersecurity, and provide practical recommendations that can help strengthen law enforcement responses to digital threats in Nigeria.

Statement of the Problem

Cybercrime has become one of the fastest-growing threats in Nigeria's digital space, affecting individuals, businesses, and government institutions. Despite the increasing reliance on digital technologies, many law enforcement agencies in the country still struggle to cope with the technical demands of investigating and managing cyber incidents. According to (Akinyetun, 2021), cybercrime cost Nigeria over $500 million in 2019, with financial institutions and government agencies among the most affected. Yet, many law enforcement personnel lack adequate training in digital forensics and often work without access to up-to-date tools or proper infrastructure. Although the Cybercrime Act of 2015 was introduced to address cyber threats legally, its enforcement remains inconsistent due to a shortage of skilled investigators and gaps in legal procedures for handling electronic evidence. (Heikkilä et al., 2021) also reported that only a limited number of forensic labs operate in Nigeria, and most do not meet global standards for digital investigations. These challenges are further compounded by weak collaboration between security agencies, which often results in delayed responses and missed opportunities for cyber threat mitigation. As cyber threats continue to evolve, there is an urgent need to assess the real capabilities of law enforcement agencies in handling digital forensic investigations and managing cyber incidents. Without this, Nigeria risks falling further behind in the global fight against cybercrime.

Research Questions

The main questions addressed by this research are:

i. What is the current performance of Nigerian law enforcement agencies in conducting digital forensic investigations and responding to cyber incidents?
ii. What challenges do law enforcement agencies face in effectively managing cybercrime and securing digital evidence?
iii. How can the collaboration between Nigerian law enforcement agencies and other?

Aim and Objectives of the Study

The aim of this research to Evaluate Law Enforcement Performance in Digital Forensics Investigation and Cyber Incident Management In Nigeria. The objectives are:

i. Assess the current performance of Nigerian law enforcement agencies in conducting digital forensic investigations and managing cyber incidents.

ii. Identify the key challenges faced by law enforcement agencies in tackling cybercrime, particularly in the areas of digital evidence collection and incident response.
iii. Propose strategies for improving inter-agency collaboration and the overall effectiveness of law enforcement in combating cybercrime in Nigeria.

LITERATURE REVIEW

Conceptual Framework

This study is conceptualized based on the key elements of digital forensics and cyber incident management within the Nigerian law enforcement context. The framework outlines the interrelated components that impact the effectiveness of law enforcement agencies in responding to cybercrimes, including infrastructure, skills, legal frameworks, and inter-agency collaboration. Figure 2.1 illustrates the core challenges and capabilities that influence the execution of digital forensic investigations and cyber incident management in Nigeria.

Digital Forensics

Digital forensics is the process of collecting, analyzing, and preserving digital evidence to support criminal investigations and legal proceedings (Majed et al., 2020). It involves the identification, recovery, and examination of data from electronic devices such as computers, mobile phones, and cloud systems. The field is essential in combating cybercrime, as it helps law enforcement agencies trace illegal activities, recover lost or manipulated data, and present admissible evidence in court. Digital forensics follows a structured approach, including evidence acquisition, analysis, documentation, and presentation. Its effectiveness depends on specialized tools, trained personnel, and adherence to legal standards. In Nigeria, digital forensics is still evolving, with law enforcement agencies facing challenges such as inadequate infrastructure, limited technical expertise, and legal constraints in handling digital evidence.

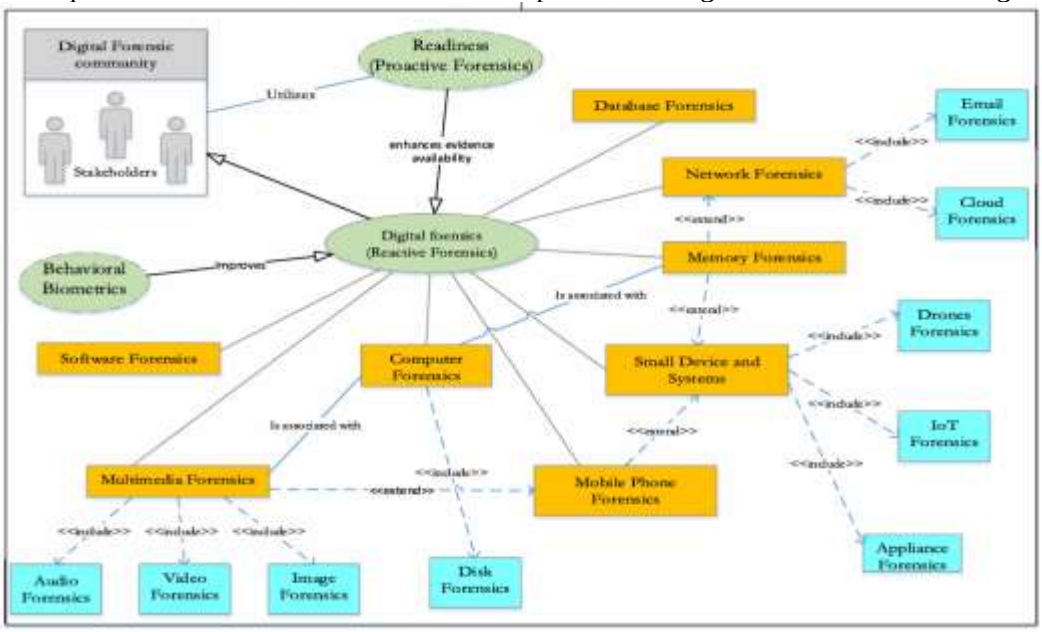

Figure 2.2: Illustration of the Various Subdomains of Digital Forensics Adopted from (Al-Dhaqm et al., 2021)

Digital Forensic Processes

A high-level digital forensics process is defined by National Institute of Standards and Technology (NIST) which consists of the following phases.

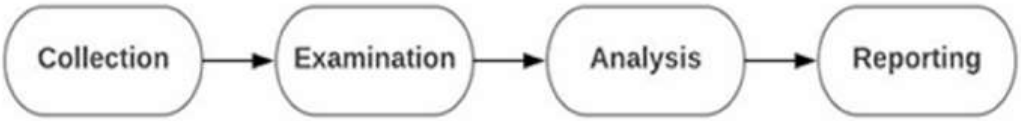

Figure 2.3: Digital Forensics Process proposed by NIST Adopted from (Dimitriadis et al., 2020)

i. Collection: This involves locating potential sources of digital evidence. Devices such as computers, smartphones, storage media, and network logs are identified based on the nature of the incident.
ii. Examination: This step focuses on securing and collecting digital data without altering its original form. Tools like write blockers are used to prevent tampering during data acquisition, ensuring the chain of custody is maintained.
iii. Analysis: The collected data is examined using forensic tools to uncover relevant facts. Analysts may look for deleted files, hidden information, communication logs, timestamps, and malware traces.
iv. Reporting: Findings are documented in a detailed and understandable format, often accompanied by screenshots, logs, and analysis results. Reports must be clear and legally sound, as they may be presented in court.

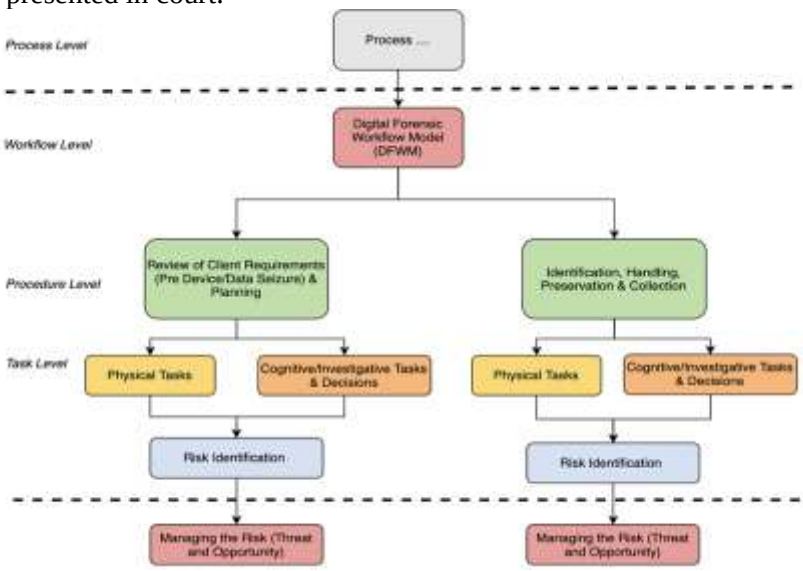

Figure 2.4: Elements of the Digital Forensic Investigation Process at Workflow, Procedure and Task Levels Adopted from (Horsman & Sunde, 2022)

Digital Forensic Tools and Relevance in Criminal Investigations

Digital forensic tools enable investigators to extract, analyze, and interpret data from a wide range of digital devices. Tools such as EnCase, FTK, Autopsy, and Wireshark help uncover hidden, deleted, or encrypted information (Singh & Kumar, 2020).

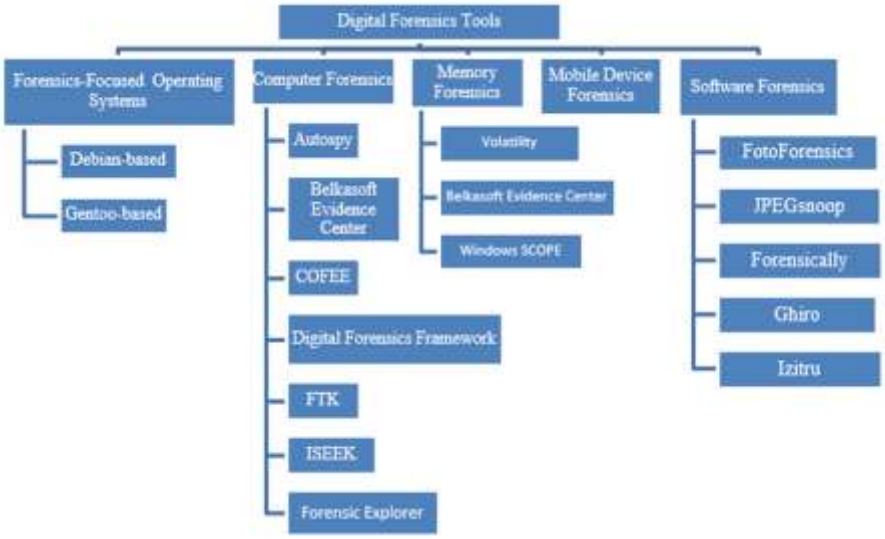

Figure 2.5: Classification of Digital Forensic Tools Adopted From (Parveen et al., 2020)

Cyber Incident Management

Cyber incident management refers to the structured process of identifying, managing, and resolving cybersecurity incidents to minimize their impact on information systems and critical operations. It is a vital aspect of an organization's or nation's cybersecurity strategy, especially as digital threats continue to grow in sophistication and frequency (Ahmad et al., 2020).

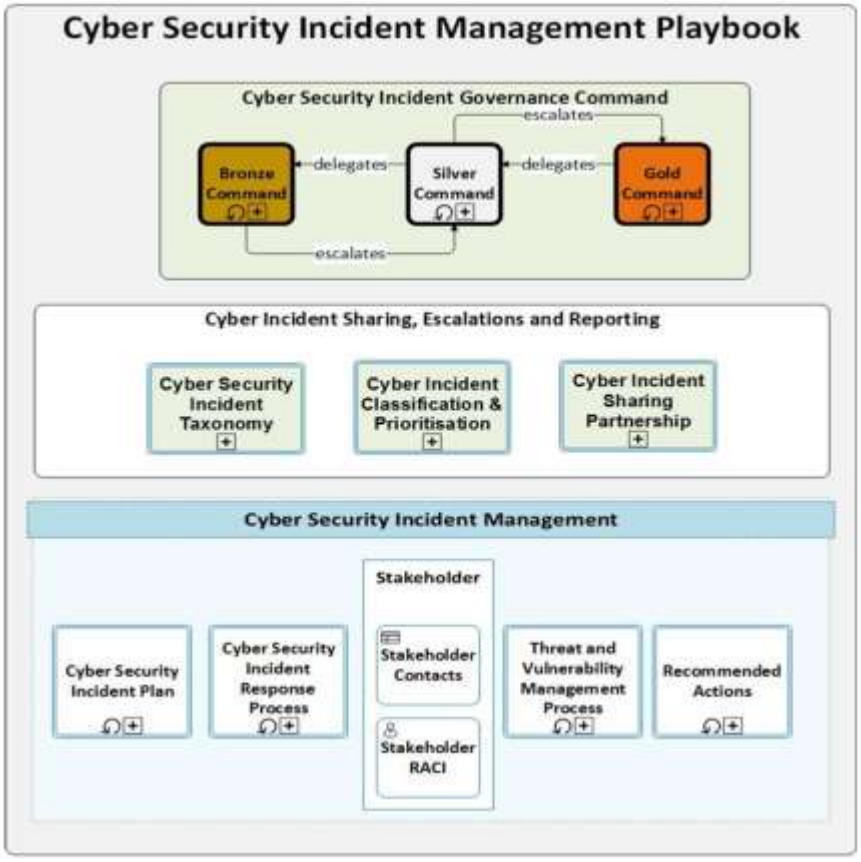

Figure 2.6: A Playbook for Managing Cyber Incidents Adopted from (C. Onwubiko, 2020)

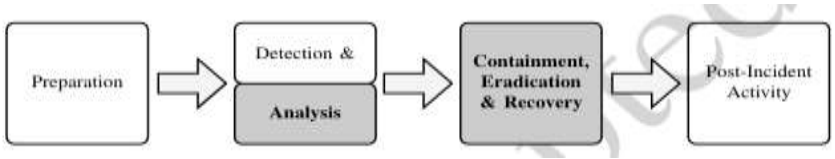

Figure 2.7: Survey focus based on NIST Incident Response Life Cycle Adopted From (Schlette et al., 2021)

In Nigeria, many institutions are still developing their capacity for effective cyber incident management. Limited funding, inadequate training, and a lack of specialized personnel continue to pose challenges. Strengthening these capabilities is essential for protecting national infrastructure, businesses, and citizens from the growing threat of cyberattacks (Ikuero & Zeng, 2022).

Law Enforcement in Cybercrime Investigation

Law enforcement agencies are central to cybercrime investigation, requiring technical expertise to trace, analyze, and prosecute offenders. In Nigeria, specialized units within the Nigeria Police Force (NPF), the Economic and Financial Crimes Commission (EFCC), and the Nigerian Communications Commission (NCC) are tasked with investigating offenses such as internet fraud, ransomware, identity theft, and data breaches (Ukasha, 2020). Despite legislative advancements like the Cybercrimes Act of 2015, investigative capacity remains constrained by a shortage of trained personnel, outdated forensic tools, inadequate funding, and weak inter-agency collaboration (Oktaviana & Clark, 2024). These challenges are particularly acute in rural and under-resourced regions, where basic digital evidence-handling tools and awareness are lacking (Ayotunde, 2025). While training programs and international partnerships have laid a foundation for improvement, sustained investment in infrastructure, capacity building, and cross-sector collaboration is essential to strengthen Nigeria's cybercrime response and restore public trust in the digital ecosystem.

Legal and Institutional Frameworks

Nigeria's legal framework for addressing cybercrime is anchored by the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, which defines and criminalizes offenses including hacking, identity theft, and fraud, and grants investigative powers to law enforcement while imposing data retention duties on service providers (George & Ngwoke, 2022). Nigeria also participates in international agreements such as the Malabo Convention and the Budapest Convention, which support cross-border cooperation in cybercrime investigations (Bouke et al., 2023).

Inter-Agency Collaboration and Capacity Building

Effective response to cybercrime and digital investigations requires strong collaboration among key stakeholder's law enforcement agencies, regulatory bodies, private sector entities, and international partners. In Nigeria, however, inter-agency coordination is often fragmented due to overlapping mandates, poor information sharing, and lack of standardized protocols. Capacity building is equally critical. While some agencies have benefited from local and international training programs in digital forensics and cyber law, these efforts are still limited in scope and consistency.

Empirical Review

(Egho-Promise et al., 2024) in their study aims to develop a comprehensive framework and improved methodologies tailored for conducting digital forensic investigations in cloud settings. A pragmatic research philosophy integrating positivist and interpretivist paradigms guides an exploratory sequential mixed methods design. Qualitative methods, including case studies, expert interviews, and document analysis were used to explore key variables and themes. Findings inform hypotheses and survey instrument development for the subsequent quantitative phase involving structured surveys with digital forensics professionals, cloud providers, and law enforcement agencies, across the globe. The multi-method approach employs purposive and stratified random sampling techniques, targeting a sample of 100-150 participants, across the globe, for qualitative components and 300-500 for quantitative surveys. Qualitative data went through thematic and content analysis, while quantitative data were analyzed using descriptive and inferential statistical methods facilitated by software such as SPSS and R. An integrated

mixed methods analysis synthesizes and triangulates findings, enhancing validity, reliability, and comprehensiveness. A key limitation of the study is its global focus, which may limit the applicability of findings to specific local contexts like Nigeria. (Apau & Koranteng, 2020) in their paper contends to the existence of legislation and mandated institutions. It concludes that, though the sector has recorded advancements over the years, the progress has been very slow leaving DFI still at an infant stage. Existing legislations are scattered and cumbersome whereas mandated institutions lack the requisite capacity. There is a need to streamline existing laws into a comprehensively harmonized legal framework. Furthermore, heavy investments must be deployed to boost the capacities of relevant institutions.

(Balogun et al., 2023) investigated the obstacles to effective fight against cyber-crime in Bauchi State Police command; as perceived by members of the public in Bauchi Metropolis. The objective is to examine the nature of cyber-crimes commonly perpetrated in Bauchi Metropolis? Theory of technology-enable crime was adopted to explain the phenomena under study. Questionnaires and in-depth interview (IDI) were used to collect the necessary data. Multi stage cluster sampling was used in selecting of 208 respondents for the study. The data was analyzed using SPSS version 22. The findings indicate that Nigeria Police lack modern technological gadgets to combat cyber-crime, lack of proper training affect the police in combating cyber-crime, the common type of cyber-crime perpetrated are ATM fraud, Hacking and internet fraud. It is recommended that police should be equipped with modern equipment like computers, internet facilities to enable them prevent and detect cyber-crime as soon as it occurs, the police should be properly trained on cyber-crime typologies in order to broaden their knowledge on the various types of cyber-crime that exist. The study is geographically limited to Bauchi Metropolis, which restricts the generalizability of its findings. Additionally, it relies heavily on public perception, which may not fully reflect the technical or institutional realities within the police force. (Kareem et al., 2025) in their paper provides a comprehensive overview of digital forensics investigations and the tools utilized in threat intelligence. As cyber threats become increasingly sophisticated, the need for effective forensic methods to analyze and respond to these threats has grown significantly. We explore various digital forensics techniques, including data acquisition, analysis, and preservation, as well as the integration of these techniques into threat intelligence frameworks.

(Aisha, 2024) highlighted that the evolution of information technology has created a parallel world in cyberspace, offering opportunities and convenience to users, but it has also paved the way for malicious actors to exploit this interconnected network. With the proliferation of netizens, the misuse of technology has led to a surge in cybercrime, both at domestic and international levels. In contrast to traditional physical crimes, modern cybercriminals can cause extensive damage and financial losses with the click of a button. These paper highlights the economic toll of cybercrime, emphasizing the impact on individuals and businesses as criminals exploit vulnerabilities to steal, defraud, and compromise sensitive data. Cybersecurity measures have become crucial in safeguarding against these digital threats, protecting the global economy from this evolving challenge. A limitation of this study is that it focuses primarily on the economic impact of cybercrime, potentially overlooking the broader social and psychological consequences for individuals and communities. (Nweke & Anim-Wright, 2024) paper presents a systematic review of the literature concerning the adoption and application of technology in policing and law enforcement in Nigeria. The rapid growth of digital technology globally has not left the policing sector untouched. Nigeria, as a developing nation, offers a unique perspective, grappling with challenges in infrastructure, digital literacy, and governance. Drawing from an array of scholarly articles, journals, and reports, this review seeks to ascertain the extent of technology-based advancements in the Nigerian policing system, its effects on crime prevention and detection, and the associated challenges.

(Onwubiko & Eboibi, 2020) highlighted that the increased use of the internet and information technology in Nigeria has led to the need to utilize technologies to identify and prosecute perpetrators of crimes. In today's world, the application of forensics in the investigation and prosecution of crimes is essential. This paper critically examines the effect of the absence of a coordinated standard for the execution and presentation of forensic investigations utilizing electronic evidence in Nigeria. It examines the nature and scope of the various forensic models proposed, while questioning the appropriateness or otherwise of their usefulness in criminal prosecutions. The paper suggests the need for the regulation of forensics

practices, the provision of standards, and a universal model for the successful prosecution of crimes in Nigeria. A limitation of this study is the lack of empirical data on the effectiveness of existing forensic models in Nigeria, which may hinder a comprehensive understanding of their real-world application. (Usman et al., 2023) examined criminal profiling and the challenges of criminal investigation in the Nigeria Police Force focusing on Kogi State Command. The specific objectives of the study included examining the mechanisms put in place to aid criminal profiling in the Nigerian criminal justice system, especially in Kogi State Police Command; an evaluation of the effectiveness of the mechanisms; identification of the challenges facing criminal profiling in the Nigerian criminal justice system, especially in Kogi State Police Command; and suggestions on how criminal profiling can be effective in the Nigerian criminal justice system.

(Chiji, 2024) analysed the evaluation of cyber policies for regulating, monitoring, and supervising cyberspace activities, along with the implementation of cybersecurity measures to address technologically advanced crime. A mixed methods strategy, including qualitative and quantitative methodologies, was employed for data collecting. The research revealed that although cyberspace provides avenues for social contact, idea exchange, information dissemination, commercial transactions, and additional activities, it remains susceptible to cyber threats including ransomware, fraud, warfare, terrorism, trafficking, and breaches of privacy. Formulating cyber regulations to regulate actions in cyberspace is crucial for efficient law enforcement, alongside the establishment of a cybersecurity framework to safeguard critical cyber systems and bolster security protocols across several sectors. To safeguard both the public and private sectors against cybersecurity risks, it is essential to create and execute plans. These tactics encompass the regular evaluation and auditing of security systems, investment in cybersecurity training programs, maintenance of current systems, formulation and rehearsal of incident response plans, and dissemination of information among experts and professionals. A limitation of this study is the potential gap between policy formulation and actual implementation, as it may not fully account for the practical challenges of enforcing cybersecurity measures in diverse sectors. Furthermore, the reliance on a mixed-methods approach might introduce biases due to the subjective interpretation of qualitative data, particularly in assessing the effectiveness of cybersecurity frameworks. (Tor, 2019) applied the doctrinal methodology to discuss human rights considerations in the investigation and prosecution of cybercrimes. It raised some questions, one of which is "whether compliance with the constitutional provisions on human rights in the course of investigating cybercrimes and indeed other crimes impede national security?" The article affirms that human rights are complementary to investigations and national security as both are mutually exclusive especially considering that the overriding basis of the criminal justice process including investigation is anchored on fairness and justice.

METHODOLOGY

Research Design

This study uses a mixed-methods approach to better understand how prepared Nigerian law enforcement is when it comes to handling digital forensic investigations and managing cyber incidents. It combines both qualitative and quantitative methods to paint a fuller picture.

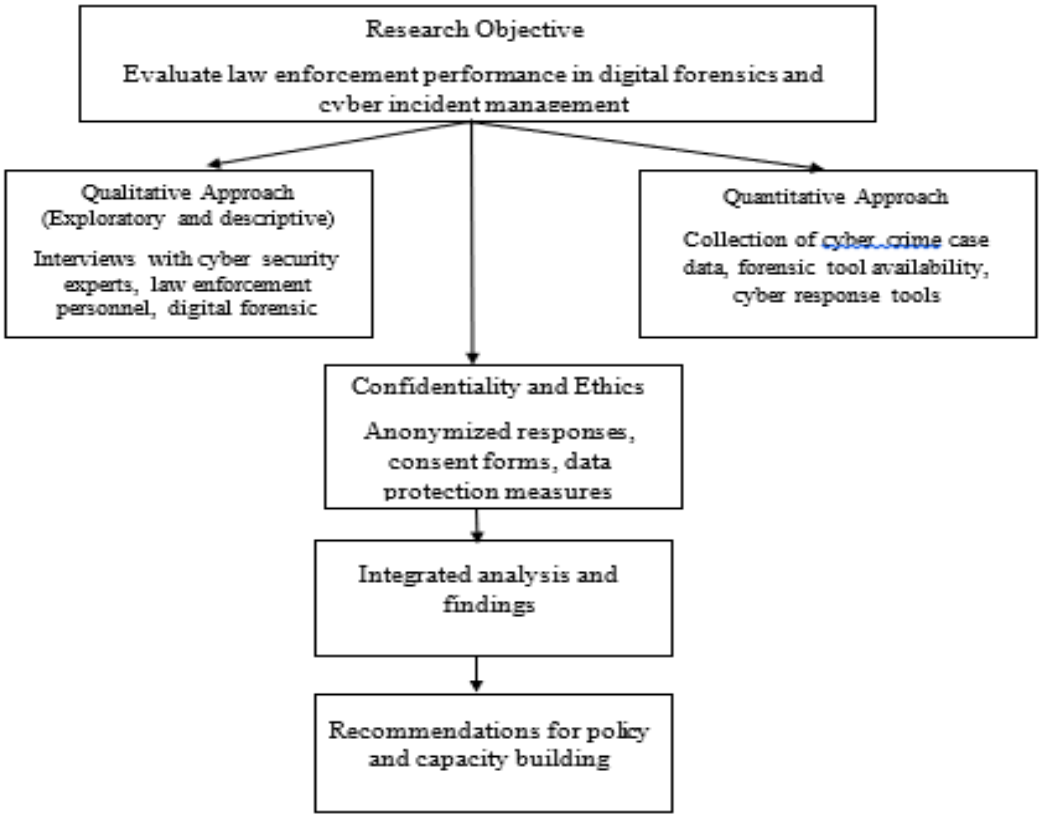

Figure 3.1: Research Design Diagram for Evaluating Law Enforcement Performance in Digital Forensic Investigations and Cyber Incident Management in Nigeria

Population, Sampling and Sampling Techniques

The study population comprises Nigerian law enforcement personnel, digital forensic experts, and cybersecurity stakeholders from public and private sectors. Purposive sampling was used to select experienced participants from key cities such as Abuja, Lagos, and Port Harcourt, ensuring diverse and context-rich insights. This approach captures varied operational environments and resource realities across Nigeria's cybersecurity landscape.

Data Collection

Both qualitative and quantitative data were collected to assess Nigerian law enforcement's performance. Semi-structured interviews with cybersecurity experts and officers provided qualitative insights, while surveys and reviews of past cybercrime cases supplied quantitative metrics on tool effectiveness and incident response. This mixed-method approach enabled a holistic evaluation of strengths, weaknesses, and areas for improvement.

Techniques for Data Analysis

Interview data was analyzed thematically, while quantitative data from surveys and case records were examined using descriptive and inferential statistics. Triangulation was employed to cross-verify findings, ensuring consistency and enhancing the reliability of the results. This approach enabled a holistic evaluation of law enforcement's digital forensics and incident management capabilities.

RESULTS AND DISCUSSION

The results of the findings are presented below:

Table 4.1: Demographic Information of Respondents

This section presents the demographic details of the respondents involved in the survey. The demographic variables include: agency affiliation, gender, age, educational qualification, years of experience, and professional role.

Table 4.1: Distribution of Respondents by Agency Affiliation

Agency	Frequency	Percentage (%)
Nigeria Police Force (NPF)	30	30.0
Economic and Financial Crimes Commission (EFCC)	25	25.0
National Information Technology Development Agency (NITDA)	15	15.0
Department of State Services (DSS)	10	10.0
Private Sector (Cybersecurity Experts)	20	20.0
Total	100	100.0

The data shows that respondents were evenly distributed among key law enforcement and cybersecurity organizations. The highest number of respondents came from the NPF 30%, followed by EFCC 25%. Inclusion of private sector professionals ensures a broader understanding of cybercrime management across institutional lines.

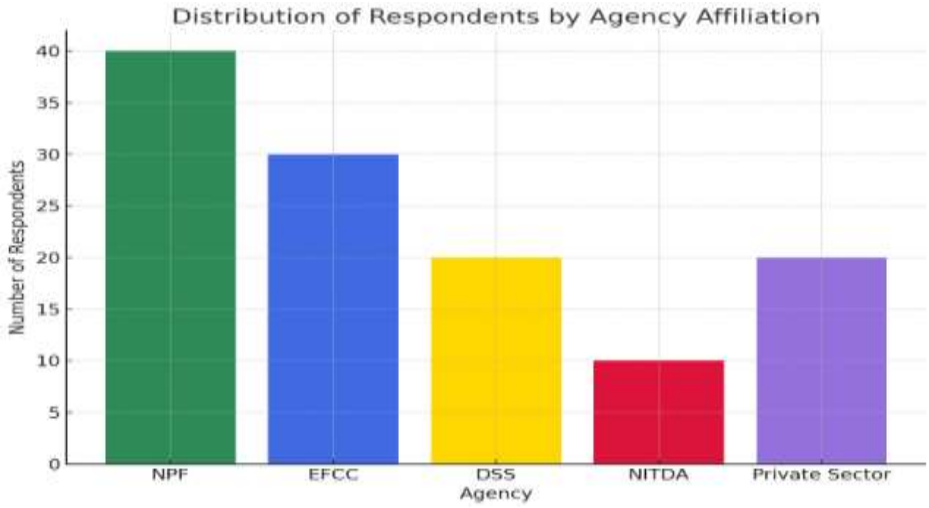

Figure 4.1: Distribution of Respondents by Agency Affiliation. It displays four bars, each representing a different agency (NPF, EFCC, DSS, NITDA).

Table 4.2: Distribution of Respondents by Years of Experience

Years of Experience	Frequency	Percentage (%)
1-3 years	18	18.0
4-6 years	32	32.0
7-10 years	25	25.0
Above 10 years	25	25.0
Total	100	100.0

A substantial proportion 50% of the respondents have more than 7 years of experience, suggesting high expertise in the field of digital forensics and cyber incident response. This lends credibility to the findings obtained through the survey.

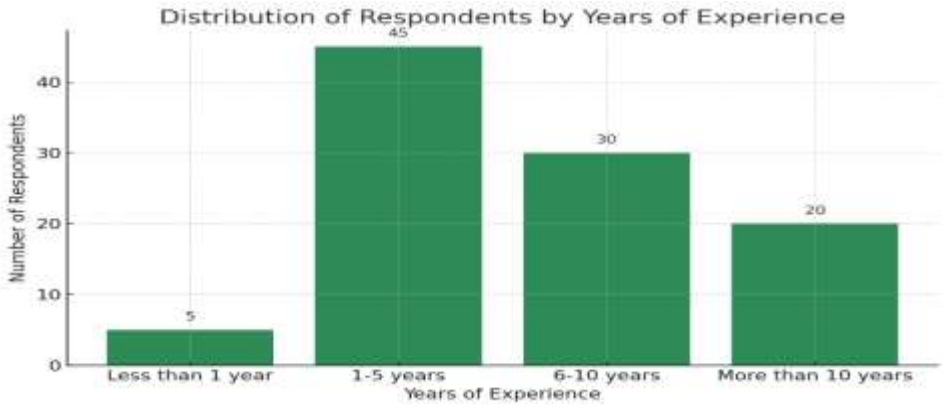

Figure 4.2: Bar Chart Showing Distribution of Respondents by Years of Experience

Overview of Respondents Experience and Background in Digital Forensics and Cybercrime Management

Table 4.3: Respondents with Formal Training in Digital Forensics

Training in Digital Forensics	**Frequency**	**Percentage (%)**
Yes	62	62.0
No	38	38.0
Total	100	100.0

Only 62% of the respondents have formal training in digital forensics. This reflects a major skill gap in law enforcement agencies which might impact their efficiency in handling cybercrime investigations.

Figure 2.3: Bar chart showing the distribution of respondents based on whether they have received training in digital forensics.

Assessment of Law Enforcement Performance

Table 4.4: Respondents Rating of Current Law Enforcement Performance in Cybercrime Investigation.

Performance Rating	**Frequency**	**Percentage (%)**
Excellent	5	5.0
Good	20	20.0
Fair	35	35.0
Poor	40	40.0
Total	100	100.0

A majority of the respondents 75% rated the performance of law enforcement in cybercrime investigation as either fair or poor. This underscores the need for strategic improvement in capacity building, forensic tools, and institutional efficiency.

Challenges Faced by Law Enforcement Agencies

Table 4.5: Major Challenges Identified by Respondents

Challenge	**Frequency**	**Percentage (%)**
Inadequate forensic tools	30	30.0
Limited training and skill gaps	25	25.0
Poor inter-agency collaboration	15	15.0
Lack of legal clarity on digital evidence	10	10.0
Funding and resource constraints	20	20.0
Total	100	100.0

Figure 2.4: Challenges Faced by Law Enforcement Agencies in Digital Forensics

Current Level of Inter-agency Collaboration

Table 4.6: Respondents Perception of Inter-agency Collaboration

Collaboration Level	Frequency	Percentage (%)
Very effective	8	8.0
Somewhat effective	28	28.0
Not effective	64	64.0
Total	100	100.0

Only 36% of respondents consider inter-agency collaboration to be effective or somewhat effective, while the majority 64% perceive it as ineffective. This aligns with the need for improved coordination among cybercrime-related bodies in Nigeria.

Discussion of Findings

The findings are discussed in relation to the three research questions that guided this study.

Research Question 1: What is the current performance of Nigerian law enforcement agencies in conducting digital forensic investigations and responding to cyber incidents?

The findings indicate that the performance of Nigerian law enforcement agencies in digital forensics and cyber incident response is still developing and faces significant challenges. This aligns with the background of the study, which highlighted the struggles of agencies to keep up with the technical demands of investigating cybercrime (Akinyetun, 2021). The quantitative data revealed that a majority of

respondents rated the performance of law enforcement as 'average' or 'poor', which is consistent with the assertion by Obamanu (2018) that these agencies are often limited by resource and structural challenges.

The qualitative data provided further insight into these challenges. For instance, the theme of 'Resource Constraints' was prominent, with one interviewee stating, "We can barely afford basic forensic imaging tools." This directly supports the background study's claim of 'outdated or inadequate forensic tools' (Obamanu, 2018) and the report by Heikkilä et al. (2021) that most forensic labs in Nigeria do not meet global standards. The lack of resources not only hampers the ability to conduct thorough investigations but also affects the morale and motivation of the personnel involved.

Research Question 2: What challenges do law enforcement agencies face in effectively managing cybercrime and securing digital evidence?

The study identified several key challenges, including 'Legal Framework Gaps' and a lack of specialized skills. These findings are in line with the background of the study, which pointed to 'unclear or not properly enforced' legal processes for handling digital evidence (Sibe & Muller, 2022). The concern raised by stakeholders about the court admissibility of digital evidence due to outdated laws directly reflects the challenges in enforcing the Cybercrime Act of 2015, as mentioned in the background.

Furthermore, the challenge of inadequate training and skills is a recurring theme. The background of the study emphasized the 'lack of specialized personnel' and 'limited access to training' (Obamanu, 2018). The findings of this study confirm that this is still a major issue. The lack of trained personnel not only affects the quality of investigations but also the ability of agencies to adapt to new and emerging cyber threats, a concern also raised by Ogundele et al. (2023).

Quantitative Analysis

To test this theory, a chi-square test was conducted between two categorical variables:

i. Formal training in digital forensics (Yes/No)
ii. Perceived performance (Excellent/Good/Fair/Poor)

Table 4.7: Cross-tabulation of Training in Digital Forensics and Performance Rating

Performance Rating	With Training	Without Training	Total
Excellent	4	1	5
Good	15	5	20
Fair	25	10	35
Poor	18	22	40
Total	62	38	100

Chi-square Test Result:

i. χ^2 (df=3) = 9.78,
ii. p-value = 0.0201

Since the p-value (0.0201) < 0.05, we reject the null theory. There is a statistically significant relationship between formal training in digital forensics and perceived performance. This implies that law enforcement personnel with relevant training are more likely to report better performance in handling cybercrime investigations.

Qualitative Analysis (Interview Insights)

Many interviewees emphasized that limited hands-on training and outdated knowledge significantly hinder performance. One cybersecurity expert from one of the security agencies noted: "Officers rely on outdated investigation models. The few who have been trained abroad or through special workshops show clear distinction in their approach and outcomes."

Research Question 3: How can the collaboration between Nigerian law enforcement agencies and other relevant institutions be enhanced for effective cyber incident management?

The findings strongly suggest a need for enhanced inter-agency collaboration. The quantitative data showed a high level of agreement among respondents that collaboration is crucial for effective cyber incident management. This supports the background of the study, which identified 'weak coordination between agencies' as a major limitation (Obidimma & Ishiguzo, 2023).

The qualitative data also highlighted the desire for a more integrated approach. The suggestion for a 'centralized cybercrime response unit' reflects the need for a more coordinated effort, as opposed to the current fragmented approach. The background of the study mentioned that agencies like the Nigerian Police Force, EFCC, and NITDA have taken steps to address cybercrime, but their efforts are often limited. Enhanced collaboration would allow these agencies to pool their resources and expertise, leading to more effective and efficient responses to cyber incidents.

Quantitative Analysis

Respondents were asked to rate how much various challenges impacted cybercrime management. A weighted average score was calculated.

Table 4.8: Mean Rating of Challenges Affecting Cybercrime Management

Challenge	Mean (Out of 5)
Inadequate forensic tools	4.5
Limited training and skill gaps	4.2
poor inter-agency collaboration	3.9
Legal ambiguity on digital evidence	3.8
Funding/resource constraints	4.0

All challenges scored above 3.5 on a 5-point scale, with inadequate forensic tools and training gaps receiving the highest mean scores (4.5 and 4.2 respectively). This indicates that these challenges are critically affecting law enforcement performance.

Theory Testing (One-Sample t-Test)

i. Test Value = 3 (Neutral Impact)
ii. $t = 9.12$, $p < 0.01$

Reject the null hypothesis. These challenges have a statistically significant impact on cybercrime management.

Qualitative Analysis (Interview Insights)

Themes identified:

i. Resource Constraints: “We can barely afford basic forensic imaging tools,” noted a senior cyber security expert.
ii. Legal Framework Gaps: Stakeholders expressed concerns over court admissibility of digital evidence due to outdated laws.

Quantitative Analysis

Respondents were asked whether improved collaboration could significantly enhance performance.

Table 4.9: Perception of Need for Improved Inter-agency Collaboration

Response	Frequency	Percentage (%)
Strongly agree	50	50.0
Agree	30	30.0
Neutral	10	10.0
Disagree	6	6.0
Strongly disagree	4	4.0
Total	100	100.0

A total of 80% of respondents agree that stronger inter-agency collaboration would improve cyber incident response, indicating high consensus.

Chi-square Goodness-of-Fit Test

$\chi^2 = 58.6$, $p < 0.001$

Reject the null hypothesis. There is strong evidence that collaboration is critically needed.

Qualitative Analysis (Interview Insights)

Recurring points include:

i. Bureaucratic boundaries prevent efficient sharing of intelligence.
ii. Lack of a centralized digital forensics database.
iii. Suggested creation of a Joint Cybercrime Response Taskforce.

DISCUSSION OF FINDINGS

The findings reveals a clear link between the challenges identified in this study and the issues raised in the background of the study. The performance of Nigerian law enforcement agencies in digital forensics and cyber incident management is hampered by a combination of resource constraints, legal and structural challenges, and a lack of inter-agency collaboration. These findings are consistent with the literature and provide empirical support for the concerns raised by various scholars in the field (Akyazi et al., 2021; Vasanthi et al., 2021).

The study, therefore, confirms the urgent need for a comprehensive approach to improving the capabilities of Nigerian law enforcement agencies in combating cybercrime. This includes investing in modern forensic tools and training, updating the legal framework to address the complexities of digital evidence, and fostering a culture of collaboration among all relevant stakeholders. By addressing these challenges, Nigeria can strengthen its cybersecurity posture and more effectively protect its digital space from the growing threat of cybercrime.

The findings also offer valuable insights into the professional landscape of digital forensics and cybercrime management in Nigeria. The analysis of respondents' years of experience revealed a concentration in the mid-career bracket (5–10 years), indicating that a substantial number of practitioners have developed considerable practical knowledge, though a notable portion also falls within the 1–4 years category. This suggests a growing and maturing workforce in the cybercrime field, which is essential for sustaining national efforts against evolving threats. Interestingly, fewer respondents possessed over 10 years of experience, which may reflect the relatively recent emergence of cybercrime as a specialized focus within the broader law enforcement and ICT communities in Nigeria. Regarding institutional affiliation, the majority of respondents were from the Nigeria Police Force (NPF) and the Economic and Financial Crimes Commission (EFCC), confirming their leading roles in cybercrime investigations and digital forensics activities. The Department of State Services (DSS) and the National Information Technology Development Agency (NITDA) were less represented, while the private sector accounted for only 20% of the respondents. This skewed distribution suggests that government agencies still dominate the cybercrime response space, potentially limiting the integration of private-sector innovation, forensic consulting, and technical expertise. The underrepresentation of private actors may hinder holistic national cyber resilience, especially in areas like threat intelligence sharing, proactive cyber defense, and advanced incident response. Furthermore, the background of respondents showed varying levels of formal training and specialization in digital forensics, with some indicating on-the-job experience rather than structured academic or professional certifications. This highlights a pressing need for standardized training pathways, continuous professional development, and investment in formal education and certification programs tailored to digital forensics and cybercrime investigation. Overall, these findings underscore the importance of multi-sectoral collaboration, capacity development, and policy harmonization to address existing gaps and strengthen Nigeria's digital forensics ecosystem. A more balanced integration of experienced personnel across sectors, supported by consistent training and inter-agency cooperation, will be crucial in tackling the complexities of modern cybercrime.

Summary

This study investigated the experience and professional backgrounds of individuals involved in digital forensics and cybercrime management across selected Nigerian agencies. It assessed the distribution of respondents by agency affiliation, years of experience, and exposure to cybersecurity-related tasks. The data revealed that the majority of respondents were affiliated with public sector institutions such as the Nigerian Police Force (NPF), Economic and Financial Crimes Commission (EFCC), and Department of State Services (DSS), while a smaller proportion came from private organizations and regulatory bodies like NITDA. The study also highlighted that most of the participants had between 1 to 10 years of experience, suggesting a relatively young but growing field. Overall, the findings underscore the evolving capacity of Nigerian institutions to respond to cybercrime, while also pointing to gaps in cross-sector participation and advanced technical expertise.

CONCLUSION

The findings of the study highlight the increasing relevance of digital forensics and cybercrime management in Nigeria, as well as the nation's gradual buildup of human capacity in these critical areas. However, the uneven distribution of experience and representation across agencies signals a lack of uniformity in training, resource allocation, and strategic alignment. Public agencies remain the dominant players in cybercrime control, but their efforts alone may not be sufficient in combating the complex and evolving nature of cyber threats. To achieve a more robust and sustainable approach, both public and private sectors must work together in a coordinated manner. The study concludes that while Nigeria is making progress, a more comprehensive, inclusive, and future-oriented strategy is required to strengthen national cybersecurity resilience.

RECOMMENDATIONS

To address the challenges identified, the study recommends that government and private sector institutions invest heavily in structured, periodic training and capacity-building programs tailored to digital forensics and cybercrime response. These programs should incorporate international best practices and be accessible to a wider pool of practitioners, including private sector players. Strengthening partnerships between law enforcement agencies, regulatory bodies, academia, and cybersecurity firms will foster knowledge exchange and promote innovation. The government should also develop and enforce national standards for digital investigations, supported by legal frameworks that enhance cooperation and data sharing. Finally, public awareness initiatives and cyber hygiene campaigns should be launched to support preventive measures and reduce the success rate of cyber-attacks across the nation.

REFERENCES

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Aisha, O. B. (2024). THE LEGAL BATTLE AGAINST CYBERCRIME IN NIGERIA : AN ASSESSMENT OF CURRENT LAWS. *Public Policy and Administration Studies Journal*, *3*(2), 1–29. https://doi.org/10.5281/zenodo.14892555

Akinyetun, T. S. (2021). Poverty, Cybercrime and National Security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2), 86. https://doi.org/10.19184/csi.v1i2.24188

Akyazi, U., Van Eeten, M., & Gañán, C. H. (2021). Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum. *Weis*, *2*(1), 1–14.

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Razak, S. A., Grispos, G., Choo, K. K. R., Al-Rimy, B. A. S., & Alsewari, A. A. (2021). Digital Forensics Subdomains: The State of the Art and Future Directions. *IEEE Access*, *9*(3), 152476–152502. https://doi.org/10.1109/ACCESS.2021.3124262

Apau, R., & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, *2*(3), 299–309. https://doi.org/10.1016/j.fsisyn.2020.10.002

Balogun, A., Afeez, L., Olayinka Balogun, A., Folorunsho Lawal, A., & Ekundayo, J. K. (2023). AN ANALYSIS OF PUSH AND PULL FACTORS OF INTERNET FRAUD AMONG SELECTED RESIDENTS OF ILORIN METROPOLIS, KWARA STATE. *Journal of Criminology and Security Studies (IJCSS)*, *32*, 1–13.

Chiji, E. (2024). Business Ecosystem & Strategy Cyber policy for monitoring and regulating cyberspace and cyber security measures for combating technologically enhanced crime in South Africa. *International Journal of Business Ecosystem & Strategy*, *6*(5), 96–109.

C. Onwubiko. (2020). SOTER: A Playbook for Cyber Security Incident Management. *Journal of Artificial Intelligence (PLOMS AI)*, *2*(3), 1–22.

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, *5*(12), 100015. https://doi.org/10.1016/j.array.2019.100015

Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A. (2024). Digital Forensic Investigation Standards in Cloud Computing. *Universal Journal of Computer Sciences and Communications*, *3*(1), 23–45. https://doi.org/10.31586/ujcsc.2024.923

Heikkilä, H., Maalouf, W., & Campello, G. (2021). The United Nations Office on Drugs and Crime's Efforts to Strengthen a Culture of Prevention in Low- and Middle-Income Countries. *Prevention Science*, *22*(1), 18–28. https://doi.org/10.1007/s11121-020-01088-5

Horsman, G., & Sunde, N. (2022). Unboxing the digital forensic investigation process. *Science and Justice*, *62*(2), 171–180. https://doi.org/10.1016/j.scijus.2022.01.002

Ikuero, F. E., & Zeng, W. (2022). Improving cybersecurity incidents reporting in Nigeria: micro and small enterprises perspectives. *Nigerian Journal of Technology*, *41*(3), 512–520. https://doi.org/10.4314/njt.v41i3.10

Kareem, A. E. A., Oduwole, O. A., Akano, I. A., & Womiloju, A. A. (2025). An Overview of Digital Forensics Investigations and Threat Intelligence Tools. *Journal of Science Innovation & Technology Research (JSITR)*, *05*(9), 1–14.

Majed, H., Noura, H. N., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*, *2*(6), 1–6. https://doi.org/10.1109/ISDFS49300.2020.9116399

Nweke, O., & Anim-Wright, K. (2024). Transition to Tech-Driven Law Enforcement in Nigeria: A Systematic Literature Review. *Journal of Humanities, Arts and Social Science*, *8*(1), 11–22. https://doi.org/10.26855/jhass.2024.01.003

Obamanu, G. V. (2018). Legal Issues And Challenges In The Admissibility Of Digital Forensic Evidence In Courts In Nigeria. *African Journal of Science Policy and Innovation Management*, *6*(8), 22–34.

Obidimma & Ishiguzo. (2023). Artificial Intelligence And Cybercrime Investigation In Nigeria: Addressing The Legal And Technical Skills Gaps. *African Journal of Criminal Law and Jurisprudence (AFJCLJ)*, *8*(2), 30–36.

Ogundele, A. T., Awodiran, M. A., Idem, U. J., Anwana, & Emem, O. (2023). Digitally Designed Forensic Procedure a Panacea to Cyber Fraud Control in Nigeria. *2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, *2*(9), 223–229. https://doi.org/10.1109/CyMaEn57228.2023.10050964

Onwubiko, D. C., & Eboibi, F. E. (2020). The application of forensics examination in crime-related prosecution: The need for standardization and a recognized model in Nigeria. *Digital Evidence and Electronic Signature Law Review*, *17*(2004), 83–93. https://doi.org/10.14296/deeslr.v17i0.5228

Parveen, A., Khan, Z. H., & Ahmad, S. N. (2020). Classification and evaluation of digital forensic tools. *Telkomnika (Telecommunication Computing Electronics and Control)*, *18*(6), 3096–3106. https://doi.org/10.12928/TELKOMNIKA.v18i6.15295

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys and Tutorials*, *23*(4), 2525–2556. https://doi.org/10.1109/COMST.2021.3117338

Sibe, R. T., & Muller, S. R. (2022). Digital Forensic Readiness of Cybercrime Investigating Institutions in Nigeria: A Case Study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force. *Proceedings of the International Conference on Research in Management & Technovation*, *34*(April), 53–57. https://doi.org/10.15439/2022m9438

Singh, S., & Kumar, S. (2020). Qualitative Assessment of Digital Forensic Tools. *Asian Journal of Electrical Sciences*, *9*(1), 25–32. https://doi.org/10.51983/ajes-2020.9.1.2372

Tor, G. (2019). HUMAN RIGHTS CONSIDERATIONS IN INVESTIGATING AND PROSECUTING CYBERCRIMES AND OTHER THREATS TO NATIONAL SECURITY IN NIGERIA. *Conference of Judicial Trainers on Cybercrime and Electronic Evidence.*, *3*(2), 173–211.

Usman, O. J., Yunusa, E., & Gomment, T. I. (2023). Criminal Profiling and the Challenges of Criminal Investigation in Nigeria Police Force Kogi State Command. *Social Science and Humanities Research*, *6*(10), 31–65.

Vasanthi, G., Sruthi, M. V, & Shanthi, V. (2021). Data Security Approach On Cyber Crime With Web Vulnerability. *Material Science and Technology*, *20*(06), 1–5. https://doi.org/10.10543/f0299.2021.41671