Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Application of Digital Forensics in Banking Security: A Situational Analysis of Nigerian Banks

[1]Akinwale Gbenusola A ,[2]Nwachukwu Oluchukwu, and [3]Ojakorotu Victor
[12]University of Lagos, Akoka, Nigeria gakinwale@unilag.edu.ng ORCID NO: 0000-0002-0290-8827
[13]Department of Political Studies & International Relations, North West University, Mafikeng, South Africa.
[3]Honorary Research Professor, Faculty of Management Sciences, Durban University of Technology, South Africa

ARTICLE INFO

Received: 25 Apr 2025

Revised: 05 Oct 2025

Accepted: 15 Oct 2025

ABSTRACT

This study examined digital forensics and criminal investigations in Nigerian Banks: Prospects, challenges, and Solutions. The specific questions were to examine the prospects of digital forensics in criminal investigations in Nigerian Banks, to investigate the challenges faced by investigators in collecting and analysing digital evidence in Nigerian Banks, to identify potential solutions to enhance digital forensic capabilities in Nigerian Banks and to explore the usefulness of digital forensics in criminal investigations in Nigerian Banks. The study used a questionnaire as the data collection instrument because of the survey method adopted in this research. In analysing data, under descriptive statistics, the data presentation involves the use of tables of frequency and percentage to analyse the responses gathered from the respondents and chi-square was used to test the hypotheses. The findings of the study discovered that digital forensics is useful in criminal investigations in Nigerian banks, and digital forensics is a recognised aspect of security intelligence operations in Nigerian banks. The study also revealed that Nigerian banks are not investing much in digital forensics, even though they have the resources to invest. The study, therefore, recommends that Banks should provide the digital forensic team with regular training on the latest technologies, tools, and techniques to stay ahead of emerging threats. Also, expose the team to the use of specialised forensics tools. Other recommendations include: increase funding for digital forensics, collaboration with other forensic bodies within and outside Nigeria to share intelligence.

Keywords: Digital Forensics, criminal investigation, Prospects, Challenges, Solutions

Background of the study

Banking in Nigeria has transformed from Branch banking operations to digital channels, leveraging technology. Digital transactions have significantly surpassed branch transactions in the Nigerian banking industry. According to recent reports, digital banking transactions have surged by 55% to N600T per annum, underscoring the sector's substantial shifts towards technological adoption. This trend is driven by the convenience, accessibility, and efficiency of digital banking services. This volume of the transactions is driven by convenience, accessibility, efficiency and by extension privacy motivates cyber criminals to always want to exploit the system to defraud the customers. This is driven more by the banks being the custodian of personal data and the funds of customers. Digital forensics is essential in Nigerian banks for several reasons, like cybercrime prevention, fraud detection, incident response, regulatory compliance, digital evidence, and risk management, among others.

The terms digital forensics, forensics computing and computer forensics are often used interchangeably (Schatz, 2007). Sindhu and Meshram (2012) defined digital forensics as the science of identifying, extracting, analysing and presenting the digital evidence that has been stored in digital devices. Various digital tools and techniques are used to achieve this.

The Nigerian Institute of Advanced Legal Studies has seen Digital forensics as a tool used in both criminal and private investigations. It is associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts. It is an investigative process. Evidence collected may be a form of intelligence gathering used for purposes other than court proceedings (for example, to locate, identify or halt other crimes). In civil litigation or corporate matters, digital forensics forms part of the electronic discovery (or eDiscovery)

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

process. However, outside of the courts, digital forensics has formed part of internal corporate investigations like in Nigerian Banks of today.

Nigeria is currently deeply enmeshed in the syndrome known as 'Cybercrime' that is being perpetrated by its nationals both within and outside the borders of the country. Its manifestation from a relatively unknown act of crime about 12 - 20 years ago has suddenly become pandemic and difficult to eradicate within the last 5 years post-COVID. In fact, the criminal code of Nigeria relating to fraud (Section 419) has become the official name for the scam mails sent by these unscrupulous elements to unsuspecting individuals and corporate entities both within and outside the borders of the country. Advanced fee fraud, which became very popular in the early 90s, served as the parent of Cybercrime (which may also be viewed to an extent as white-collar crime) practices with mainly unemployed people as its practitioners, despite the presence of anticorruption agencies. It is worth noting that Cybercrime has been of great benefit to its practitioners and their benefactors, while being dysfunctional to the victims of the scammers, their dependents, and to a large extent, the Nigerian society. Today, it has become an image nightmare for the country and its nationals.

The increasing use of technology in financial institutions like banks has led to a rise in cybercrime and financial fraud, making digital forensics a critical component of criminal investigations in Nigerian Banks. The Banks have become targets of cybercrime because of two key components of their existence customer funds and personal data data) which are motivators for the cyber criminals. Digital forensics involves the collection, analysis, and preservation of digital evidence, which can be used to investigate crimes and bring perpetrators to justice.

Current Study

Nigeria has made appreciable progress in prosecuting criminals. This has been made possible with the introduction and enforcement of the Evidence Act, which is meant to ensure that individuals or corporate bodies do not just suffer without proper evidence to ensure that justice is served. The Nigerian Institute of Advanced Legal Studies has observed that the focus of digital forensics investigations is to recover objective evidence of a criminal activity (actus reus) as well as information readily available to assist the courts in their adjudicatory process.

Tendering of electronically generated evidence before the Evidence Act of 2011 was usually as contentious and acrimonious as the litigation itself, with the opposite party usually relying on the hearsay rule, among other forms of objections under the old Evidence Act 1990 to prevent the admission of such evidence however the legislature has tried to correct some of the difficulties that the admissibility of electronically generated evidence encounters in Nigerian Courts. This form of evidence is now recognised under the Evidence Act 2011, and conditions for its admissibility are expressly provided.

Digital forensics has become a predominant field in recent times, and courts have had to deal with an influx of related cases over the past decade from Nigerian banks due to cybercrime. As computer/cyber-related criminal attacks become more predominant in today's technologically driven society, like the Nigerian financial industry, the need for and use of digital evidence has increased. There is an urgent need to hold perpetrators of such crimes accountable, successfully investigate and prosecute them. The process used to acquire this digital evidence is called digital forensics. The procedures currently used in the digital forensic process were developed focusing on areas of the digital evidence acquisition process. This has resulted in very little regard being made for the core components of the digital forensics field, for example, the legal and ethical, along with other integral aspects of investigations. This is because digital forensics, like other forensics disciplines, must ensure that the evidence (digital evidence) produced from the process can withstand the rigours of a courtroom. Digital forensics is a new and developing field, even in Nigerian Banks, still in its infancy when compared to traditional forensics fields such as botany or anthropology. Over the years, development in the field of digital forensics has been tool centered, being driven by commercial developers of the tools used in the digital investigative process. This, along with having no set standards to guide digital forensics practitioners operating in the field within the country has led to issues regarding the reliability, verifiability and consistency of digital evidence when presented in court. Hence, against this backdrop, this study seeks to examine the role of digital forensics in criminal investigations in Nigerian banks with a focus on identifying prospects, challenges, and solutions. The study will explore the application of digital forensics in investigating cybercrimes and financial frauds, and the impact of digital evidence on criminal investigations. The specific questions are to:

1. Examine the prospects of digital forensics in criminal investigations in Nigerian Banks.
2. Investigate the challenges faced by investigators in collecting and analysing digital evidence in Nigerian Banks.
3. Identify potential solutions to enhance digital forensic capabilities in Nigerian Banks.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Explore the usefulness of digital forensics in criminal investigations in Nigerian Banks.

Literature Review

The terms forensics and forensic science are often used interchangeably, and both have become popular in many disciplines. This could pose a problem if forensics is seen in its narrower scope as dealing with physical evidence as opposed to forensic science, which encapsulates a wider range of evidence, including digital and engineering entities. Though forensics may be simply defined as the application of a scientific methodology in the legal system, Casey (2004) outlines forensics as being "a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based on proof (or high statistical confidence)". Any field thus purporting to be an arm of forensics, such as digital forensics, must have as its main aim the collection, preservation and analysis of evidence to be presented in a court of law. The word sciences in "forensics sciences" originally referred to engineering, which would be used for the identification and examination of structural designs, chemistry, for the identification and examination of explosives and biology (probably the most popular) for the identification and examination of blood (DNA). Forensic science may also be and has been applied in several fields, including but not limited to meteorology, geology, anthropology and biology White, 2010). This 'forensic science net' has recently been expanded to include computer science for the identification and analysis of digital evidence. Forensic science is an investigative technique that involves using scientific methodology to uncover and gather evidence from the scenes of crime for use in the court of law.

The prevalent use of computers and its related digital technologies have become increasingly popular (Nance, 2009). These devices are increasingly being used to assist in committing traditional crimes in new ways as well as to commit a whole new set of crimes (digital crimes).

Digital Forensics is the branch of forensic science that has emerged to deal with the characteristics of legal evidence found in/using computers and other digital devices. This is an investigative technique used mainly to uncover and gather evidence on computer crimes such as hacking, computer-related fraud and identity theft. This increase in the use of digital devices in the last two decades has changed the scope of the traditional crime scene as well as created an additional type of crime scene, especially within the banking sector. The digital crime scene consists of all digital devices and other related physical evidence that may exist. These digital devices may contain traces of digital footprints, which may be reproduced into digital evidence to be used in courts. The extensive inclusion of digital evidence in the courts promotes the need for exploration of the legal context in which digital forensics falls.

Saferstien (2009) defines forensics as "the application of science to the detection, examination and presentation of evidence in legal proceedings". Some fields apply forensic science. These include but are not limited to physics, chemistry, toxicology and accounting. These fields all provide a physical context by which to understand the evidence. Digital evidence on the other hand exists in a different context to these other forms of evidence. Digital evidence exists 'digitally' in the form of electronic pulses, zeros and ones. This difference means that its acquisition, analysis, interpretation and presentation is seen differently in court.

As with other types of forensic evidence, proper standards and procedures must be followed to be admissible and considered reliable in a court of law. Casey (2004) states, "Digital investigators do not have a systematic method for stating the certainty they are placing in the digital evidence that they are using to reach their conclusions". The methodologies and tools used by digital forensic investigators worldwide have been variable, and there is no one internationally accepted benchmark that is used to acquire digital evidence through the digital forensics process. This issue is further highlighted by (Fulbright & Jaworski, 2006) where they state, "The number one problem in current litigation is the preservation and production of digital evidence". There are a number of tools, models, methodologies, guidelines and frameworks available to carry out the digital forensics process; however, there is no standardised format in place.

The mere quantity of digital information that may exist on any computer, other digital device or network presents the digital forensic investigator with a myriad of challenges. Digital evidence presents challenges, as it is inherently different from other types of evidence that may be acquired from forensic investigations in other fields. The main differences include the fact that digital evidence can be easily reproduced and manipulated by investigators and others involved maliciously or accidentally.

Digital Forensics in Banking

Digital forensics in banking is a crucial aspect of cybersecurity that involves the collection, analysis, and presentation of digital evidence to investigate and prevent financial crimes. Here is an overview of the key concepts and techniques. Digital Forensics Techniques are Automated Analysis: AI- powered tools automate the analysis of datasets, reducing investigation time and enhancing accuracy. Anomaly Detection: AI identifies

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

unusual patterns and behaviours, helping detect insider threats and advanced persistent threats (APTs). Machine learning algorithms analyse data, recognise patterns, and predict potential threats. Investigating data stored in cloud environments requires specialised tools and techniques.

The Application in Banking is Fraud Detection: AI-powered systems detect and prevent fraudulent activities, such as phishing, ransomware, and malware attacks. Incident Response: Digital forensics helps banks respond to security incidents, minimising damage and ensuring compliance with regulatory requirements. Risk Management: Digital forensics informs risk management strategies, identifying potential vulnerabilities and threats.

It comes with various Benefits and Challenges, which include AI-powered tools that enhance the accuracy of digital forensic investigation, Automation and Machine learning that streamline the investigation process. Digital forensics helps banks to comply with regulatory requirements, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCIDSS). Evolving Threats: Digital forensics helps the bank to adapt to evolving cyber threats, including AI-powered attacks and deepfakes.

The common examples of Digital Forensics in Banks are the implementation of AI-based fraud detection systems to protect customers from fraudulent activities JPMorgan Chase, First Bank Nigeria. Leveraging AI-powered analytics to combat financial crime and fraud across its global operations, HSBC. Utilise AI and machine learning algorithms to detect and prevent fraudulent transactions in real-time Paypal, First Bank Nigeria.

Digital Forensics in Nigerian Banks

Digital forensics in Nigerian banks has gained significant attention in the last decade due to the increasing threat of cybercrime and electronic fraud, leading to the top Nigerian banks making huge investments within the digital forensic functions of the banks. The Central Bank of Nigeria (CBN), through their regulations, has also encouraged the banks and other Financial Institutions (FI) to leverage digital technology in fighting cybercrime and electronic fraud. The current state of digital forensics in Nigeria includes the following:

Forensic Accounting: Studies have shown that forensic accounting plays significant role in fraud detection and prevention in Nigerian banks. Techniques such as conducting investigation, analysing financial transactions, and reconstructing incomplete accounting records have been effective in detecting financial fraud.

Digital Forensic Tools: Research has highlighted the importance of digital forensic tools in detecting and preventing cybercrime and financial fraud in Nigerian banks.

Technology–Based Forensic Auditing: Auditing studies have revealed that technology-based forensic auditing contributes significantly to financial crime detection in Nigerian banks. It is recommended that Auditors should stay abreast of updates on technological forensic auditing tools and step up their financial intelligence skills.

Biometric Authentication: Some experts have suggested that advanced biometric authentication, such as fingerprinting, can help prevent higher-value fraud and protect billions of Naira in realtime authentication.

Digital Forensics Tools

Digital forensics tools are the actual drivers of the digital forensics industry, as without them, a cybercrime or computer crime investigation cannot be carried out. The tools have, for the most part, been reliable and produce results that have been used in courts. This, despite there being no evidence of the practitioner using them being provided with in-depth information on how the tool works or the methods they employ, enabling them (practitioner) to be able to verify the authenticity of the evidence received. Digital forensics tools are classified based on their role in the digital forensics process, and the specific devices are developed for a specific operating system. The roles include evidence acquisition tools, tools for examining the evidence, evidence analysis tools and integrated tools. The following is a description of the different groups of tools, giving examples. There are a number of digital forensics tools available, developed by various organisations and groups with different objectives. Even though these tools drive the technical development of the digital forensics field, they also demonstrate or reinforce the ad hoc manner with which the field operates. There are a number of these tools available online free of charge, and they are often the tools used in training. This leaves the field open to a number of disparities. This research aims to address a number of issues existing in the digital forensics field, including those of the tools used throughout the training of practitioners. Section 2.5 discusses some existing issues in the field with regard to education.

Digital Forensics Education

While other forensic fields have a defined educational structure, digital forensics has not achieved maturity, and hence, there is a clear absence of such a framework. Despite being in its development stages, there are several other associated factors, including the challenge that practitioners working in the digital forensics field

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

come from a wide and diverse set of backgrounds, and that the field itself is driven by tool development, rather than a wider multi-disciplinary focus. These two factors present an enormous challenge to the emergence of digital forensics as an academic discipline. A major factor in enabling the acceptance of Digital Forensics as a discipline is having a structured approach to educating practitioners in the field. Yanisec, (2003) states; "a key step to improving forensics techniques lies in creating a comprehensive approach to forensics education". The educational aspect of a field undoubtedly lies in research and education. As the demand for practitioners increases so does the demand for training and education in the field at all levels. The forensic sciences, however, do not only require practitioners to have appropriate training and education, but also to be able to communicate the results clearly to a court which may contain a lay jury (Yansic, 2003). For some, Digital forensics is a purely technical field, and there is a need to refocus this thought and ensure that education and training in the field encompasses all facets. Craiger (2007) states, "There is a common misconception among laypersons that digital forensics is primarily a technical field, dealing with computers and networks". To this end academics, in designing training courses at all levels, must ensure that all facets of the field are compensated for. Craiger (2007) continues, although digital forensics does require a good deal of technical skills, it is just as important that students understand the legal basis for their actions". The importance of designing a curriculum that integrates all aspects of Digital forensics cannot be over emphasized. Education is an important factor in carving the way forward for digital forensics becoming a true forensics discipline. One of the critical factors is the widespread growth of cyber-crimes which has prompted increased concerns. Some of the challenges cited in the fighting of technology related criminal activities included along with lack of standards, is the lack of education and training standards and adequate capabilities within law enforcement Wolf (2009). Kessler (2008) notes that the computer forensics community is concerned with the lack of education and training standards for digital forensics, a point which is supported by (Rogers and Siegfried 2004). With the continued impact of technologically related crimes on our society several educational institutions have begun to develop digital forensics programmes.

Many practitioners in the digital forensics field have recognized that digital evidence is proving to be an integral part of cases being presented in courts, despite the origin of the case. Casey (2011), Hewling (2011), have made such observations in a published work. The growing popularity of these new phenomena is proving a challenge to courts and thus the practitioners in the field must be concise in their practice. An integrated framework of standards encompassing all facets of the field with a step-by-step methodology that is designed incorporating these facets assists practitioners to be more concise and observe all possibilities while conducting their practice. The work presented in this research was designed to address these issues.

Huebner (2007) indicates that the first criminally prosecuted computer crime case was in 1966. They continue noting that the first computer forensic training course was in 1989 while the first specialized software tool emerged in the 1980s. Despite this wealth of history there is still no consensus on the exact meaning of related terms, including what digital forensics is, or what cybercrime is.

These designs all focus on different aspects of the digital forensics process and do not cover all the required steps of a forensics investigation.

Method

The study population consist of those who are in the Digital and Forensic team of First Bank, United Bank for Africa, Zenith Bank, Guaranty Trust Bank and Access Bank. They are the top 5

Nigerian Banks. Also included in the sample size are the IT Control, E-Business Control, Internal Audit, Fraud Management, and Security Operations (SOC) teams of these top five (5) banks in Nigeria. Gender of the respondents shows that 90(60.0%) are male, while 60(40.0%) of the respondents are female. Information on the age of respondents shows that 40(26.7%) of the respondents fall into the age group of 20-30 years, 60(40.0%) of the respondents are in the age group of 41-50years, while 50(33.3%) are in the age bracket 41-60 years. Information on marital status shows that 59(39.3%) of the respondents are single, while 91(60.7%) of the respondents are married. This shows that most of the respondents are married. Data on ethnic groups shows 60(40.0%) of the respondents are Yoruba, 55(36.7%) of the respondents are Igbo, 10(6.7%) of the respondents are Hausa, while 25(16.7%) of the respondents belong to other tribes.

Sampling Procedure and Sample Size

The sample population is made up of staff of the top 5 Nigerian banks are First Bank, United Bank for Africa, Zenith Bank, Guaranty Trust and Access Bank, in the following teams: Digital & Forensic, IT Control, E-Business Control, Internal Audit, Fraud Management and Security Operation Centre. From the entire population, a sample is taken from different categories was used to achieve the study objectives. The total sample size of 150 were selected using convenience sampling method, 30 employees from each bank spread across the departments.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Sampling Distribution Table

NIGERIAN BANK	SAMPLE NUMBER
First Bank	30
United Bank for Africa	30
Zenith Bank	30
Guaranty Trust Bank	30
Access Bank	30
TOTAL	150

Source: Field Survey, 2025

Data Collection Instrument and Validation

The study used questionnaire as the data collection instrument because of survey method adopted in this research. The essence of instrument construction is the systematic collection of information and systematic analysis of such information. Interviews conducted with relevant stakeholders, including bank officials from E-Business Control team, Audit, Security Operations Centre (SOC), E-Fraud, Internal Control, Investigators etc, also documentary evidence and lastly observation.

Method of Data Analysis

The method for analysing the data obtained from this study includes simple percentages and chisquare. This involves analysing the data obtained during the study; the data will be presented using a simple frequency table and expressed as percentages to further simplify the analysis. Taking cognisance of the categorical nature of respondents' views from the questionnaire, the chi-square

Data Analysis / Findings

Information on the highest educational attainment revealed that 31(20.7%) of respondents are forensic experts, 31(20.7%) of the respondents have a master's qualification, 62(41.3%) of the respondents have a degree/Certification, while 26(17.3%) of the respondents have their Diplomas. This shows that most of the respondents are graduates and above.
Information on working experience, 8(5.3%) have worked for less than a year, 102 (68.0%) have worked for 5-10years, while 40(26.7%) have worked for 11 years and above.
Information on Forensic Training showed that 60(40.0%) have received basic forensic training, 50 (33.3%) have received medium-level forensic training, while 40 (26.7%) received advanced forensic training. This shows that a good number of respondents have received more than basic forensic training.
Information On Digital Forensics and Criminal Investigation: Challenges, Prospects and Solutions.

Variables/Attributes	Frequency Distribution	Percentage (%)
Do you know about digital forensics in criminal investigation?	Yes - 144 No - 06	96 04
Which aspect of digital forensic investigations are you involved in?	□Open Computer Forensics -124 □Architecture. - 8 □CAINE. - 0 □X-Ways Forensics. -0 □SANS Investigative Forensics - 0 □Toolkit – SIFT. - 0 □ EnCase. -18 □Registry Recon.- 0 □The Sleuth Kit. - 0 □Digital Forensics Framework. - 0 □Finger prints - 0 □ Others - 0	82.7 05.3 0 0 0 0 0 12.0 0 0 0 0 0 0
Is digital forensics a recognized aspect of Security Intelligence operations in your Bank?	Yes -142 No - 08	94.7 05.3

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Does your bank recognize Digital/electronic forensic evidence in investigation and litigation processes?	Yes - 143 No -07	93.3 06.7
If yes, how often is this carried out?	◻ Regularly - 140 ◻ Rarely -10 ◻ Sometimes- 0	95.3 04.7 0
Has digital forensics been useful in criminal investigation in your bank?	◻ Yes - 141 ◻ No -09	94.0 06.0
Does your bank use digital forensic approaches in crimes that involve electronic transactions only?	◻ Yes -145 ◻ No - 05	96.7 03.3
If yes, how regularly is this being carried out	◻ Regularly - 145 ◻ Rarely - 05 ◻ Sometimes -0	96.7 03.3 0
If No, what other non-electronic activities are digital forensics applied to in your bank?	◻ Finger prints - 10 ◻ Foot prints -0 ◻ Images - 60 ◻ Signature - 80 ◻ Hand writing - 0 ◻ Others -0	06.7 0 40.0 53.3 0 0
Does your bank have a specialized department for digital forensics	Yes -140 No - 0 Not Sure - 10	93.3 0 06.7
If yes, for how long has the department existed?	◻ Less than 5 years - 80 ◻ Above 5years - 70	53.3 46.7
Are digital evidence investigations part of the procedure for the bank?	◻ Yes - 142 ◻ No - 08	94.7 05.3
Are there experts or recognized digital forensic laboratories in the bank to validate electronically generated criminal evidence?	◻Yes – 100 ◻ No - 41 ◻ Not sure - 09	66.7 27.3 06.0
Is digital forensics evidence used by the bank in carrying out their criminal investigation?	◻Yes - 140 ◻ No -0 ◻ Sometimes - 10	93.3 0 06.7
Are there noticeable challenges in using digital forensics in carrying out your criminal investigation relating to electronic crimes within the bank?	◻-Yes - 96 ◻ No - 34 ◻ Sometimes -20	64.0 22.7 13.3
Has digital forensics been able to provide enough evidence to convict or exonerate the accused during investigation in your bank?	◻ Yes -100 ◻ No - 09 ◻ Sometimes - 41	66.7 06.0 27.3
If yes, how regularly has the accused been justified or convicted because of digital evidence of their involvement in the crimes?	◻ Regularly - 120 ◻ Rarely - 20 ◻ Sometimes -10	80.0 13.3 06.7
Which aspect of digital forensics has been more	◻ Open Computer Forensics - 124	82.7

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

helpful in criminal prosecution or investigation	□ Architecture. - 08 □ CAINE. ... □ X-Ways Forensics. ... □ SANS Investigative Forensics □Toolkit – SIFT. ... □ EnCase. - 18 □ Registry Recon. ... □ The Sleuth Kit. □ Digital Forensics Framework.	05.3 0 0 0 0 0 12.0 0 0 0 0
Which aspect of digital forensics is widely used in investigating crimes in your bank?	□ Open Computer Forensics - 124 □ Architecture. - 08 □CAINE. ... □X-Ways Forensics. ... □SANS Investigative Forensics □Toolkit – SIFT. ... □ EnCase. - 18 □ Registry Recon. ... □ The Sleuth Kit. □ Digital Forensics Framework	82.7 05.3 0 0 0 0 0 12.0 0 0 0
Does your bank have a Forensic team?	□Yes -140 □ No - 07 □ Not sure - 03	93.3 04.7 02.0
If yes, how many staff are in the team:	□ 5 or below - 90 □ Above 5 but less than 10 - 50 □ 10 or above - 10	60.0 33.3 06.7
Do you think that your management will continue to expand the Forensic team and operation within the Bank?	□Yes - 120 □ No -20 □ Not sure - 10	80.0 13.3 06.7
Do you think that your management can consider training more staff to expand the Forensic operation within the Bank?	□Yes - 120 □ No - 20 □ Not sure -10	80.0 13.3 06.7
As a professional, do you see the prospects of Forensic science expanding within the Nigerian banking industry?	□Yes - 130 □ No - 05 □ Not sure - 15	86.7 03.3 10.0
What do you think will be the solution to problems faced by Forensic science within the Banking industry in Nigeria?	□ More Training - 67 □ Infrastructure/Tools - 11 □ Enhanced pay for the staff - 20 □Central Bank regulation - 30 □ Collaboration with Forensic institutes - 20 □ Increased budget - 02	44.7 07.3 13.3 20.0 13.3 01.3

Source: Field Survey, 2025.

Information on whether they know about digital forensics in criminal investigation, 144(96.0%) of the respondents claimed to know about digital forensics in criminal investigation, while 6(4.0%) of the respondents claimed not to know.
Information on the aspect of digital forensic investigations they are involved in, 124(82.7%) agreed to have been involved in Open Computer Forensics, 8(05.3%) agreed to have been involved in Architecture, while 18 (12.0%) agreed to have been involved in Encase. Information on whether digital forensics is a recognised aspect of Security Intelligence operations in your Bank? 142(94.5%) claimed that digital forensics is a recognised aspect of security intelligence operations in their bank, while 8(5.3%) stated otherwise. The data shows that 143(95.3%) of the respondents confirmed that their bank recognises digital/electronic forensic evidence in investigation and litigation processes, while 07(4.7) stated otherwise. The data also showed that 141 (94.0%) confirmed that digital forensics has been useful in criminal investigations in your bank, while 09(6.0%) stated otherwise.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

145 (96.7%) of the respondents said that their bank uses digital forensic approaches in crimes that involve electronic transactions only, while 10(3.3%) stated otherwise. Information on what other non-electronic activities are digital forensics applied to in your bank, 10 (6.7%) claimed fingerprints, 60(40%) stated images while 80 (53.3) said signatures. Information on whether the bank has a specialized department for digital forensics, 140 (93.3%) said 'yes' while 10 (6.7%) said 'no', 80(53.3%) said that the specialized has existed for less than 5years while 70 (46.7%) said that it has existed for 5years or more.
Information from the survey showed that 80 (53.3%) stated that specialized department for digital forensics has existed for less than 5 years, while 70 (46.7%) stated that the department has existed for more than 5 years.
On whether there are experts or recognised digital forensic laboratories in the bank to validate electronically generated criminal evidence, 100(66.7%) said "yes", 41(27.3%) said "no" while 09(06.7%) said that they are "not sure".
On whether the management can consider training more staff to expand the Forensic operation within the Bank, on whether digital forensics evidence is used by the bank in carrying out their criminal investigation, 140 (93.3%) said "yes", while 10(06.7%) said 'sometimes"
On whether there are noticeable challenges in using digital forensics in carrying out your criminal investigation relating to electronic crimes within the bank, 96 (64.0%) said "yes", 34 (22.7%) said "no" while 20 (13.3%) said "sometimes" On whether digital forensics has been able to provide enough evidence to convict or exonerate the accused during investigation in your bank, 100 (66.7%) said "yes", 09(06.0%) said "no" while 41(27.3%) said "sometimes".
On how regularly the accused has been justified or convicted because of digital evidence of their involvement in the crimes, 120 (80.0%) said "regularly", 20(13.3%) said "rarely", while 10 (06.7%) said "sometimes".
Information on the aspect of digital forensic investigations they are involved in, 124(82.7%) agreed to have been involved in Open Computer Forensics, 8(5.3%) agreed to have been involved in Architecture, while 18 (12.0%) agreed to have been involved in Encase.
On which aspect of digital forensics is widely used in investigating crimes in your bank, 124 (82.7%) respondents said Open Computer Forensics, 8(5.3%) said Architecture, while 18 (12.0%) said Encase.
On whether the Bank has a Forensic team, 140 (93.3%) said "yes", 07(04.7%) said "no", while 03(02.0%) said "not sure".
On the number of staff in the Forensic team, 90(60.0%) responded that they have 5 or fewer staff in the team, 50 (33.3%) responded that they have more than 5 but less than 10 staff in the team, while 10(06.7%) responded that the staff have 10 or more years.
On whether the management will continue to expand the Forensic team and operation within the Bank, 120(80.0%) said 'yes', 20(13.3) said "no", while 10(06.7%) said 'not sure"
On whether the management can consider training more staff to expand the Forensic operation within the Bank, 120(80.0%) said 'yes', 20(13.3) said "no", while 10(06.7%) said 'not sure" On whether they see the prospects of Forensic science expanding within the Nigerian banking industry, 130(86.7%) said "yes", 05(03.3%) said "no", while 15(10.0%) said "not sure"
On what they consider will be the solution to the problems faced by Forensic science within the Banking industry in Nigeria, 67(44.7%) recommended more training, 11(07.3%) suggested infrastructure/tools, 20(13.3%) said enhanced pay for the staff, 30(20.0%) suggested enhanced Central Bank regulation, 20(13.3%) recommended collaboration with Forensic institutes while 02(1.3%) recommended increased budget for Digital Forensics within the Bank.

Hypotheses Testing:
H_1: Digital forensics will be significantly useful in criminal investigations in Nigerian Banks

Table 2: Relationship between Digital forensics and criminal investigation in Nigerian Banks

Does your bank recognize Digital/electronic forensic evidence in investigation and litigation processes?	Has digital forensics been useful in criminal investigation in your bank?		**Total**
	Yes	No	
Yes	136 (95.1%)	7 (4.9%)	**143**(100.0%)
No	5 (71.4%)	2 (28.6%)	**7**(100.0%)
Total	**141(94.0%)**	**9(6.0%)**	**150(100.0%)**
X2 value= 6.633 df =1 P-value = 0.010			

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

As seen above, the chi-square value is 6.633 with the degree of freedom of 1, while the p-value is 0.010, which is less than the level of significance of 0.05; we reject the null hypothesis and accept the alternative hypothesis; hence, we conclude that Digital forensics has been useful in criminal investigation in Nigerian Banks.

Discussion of Finding

This project examined the digital forensics and criminal investigation in Nigerian banks – prospects, challenges and solutions. The objectives of the research include:

To examine the prospects of digital forensics in criminal investigations in Nigerian banks: The study has shown clearly that digital forensics in criminal investigations in Nigerian banks has several prospects, including:

Enhanced Fraud Detection and Prevention: Digital forensics can help detect and prevent financial fraud by analysing digital evidence, identifying patterns of fraudulent activity, and tracing financial transactions.

Improved Investigation efficiency: Digital forensics can reduce the time spent on investigations and improve the ease of investigation, enabling banks to respond rapidly to security incidents.

Increased conviction rates: Digital forensics can provide legally admissible evidence, increasing the number of convictions in financial crimes.

Risk Management: Digital Forensics can help banks identify vulnerabilities and weaknesses in their cybersecurity infrastructure, enabling them to improve their security procedures and prevent future occurrences.

Regulatory Compliance: Digital Forensics can aid the banks in complying with the regulatory requirements, such as the Nigeria Data Protection Act and the Central Bank of Nigeria Cybersecurity guidelines.

To investigate challenges faced by investigators in collecting and analysing digital evidence in Nigerian banks: Investigators in Nigerian banks face several challenges when collecting and analysing digital evidence, including. Authenticity and Integrity: Ensuring digital evidence is genuine and not tampered with is crucial. Investigators must verify the origin and accuracy of the digital evidence. Chain of custody: Maintaining a clear and unbroken chain of custody is essential to demonstrating that digital evidence hasn't been tampered or mishandled. Limited Forensic Capacity: Law enforcement agencies in Nigeria often lack sufficient digital forensic resources, hindering effective evidence gathering and analysis. Privacy Concerns: Investigators must balance thorough investigations with the individual right to privacy, ensuring that data collection is necessary and proportionate. Technical Complexity: Digital evidence requires specialised knowledge and tools to collect, analyse, and preserve. Investigators in the banks need to stay up to date with evolving technologies. Digital Literacy: Limited awareness and technical competence among practitioners hinder effective digital evidence handling.

To identify potential solutions to enhance digital forensic capabilities in Nigerian banks: Enhancing digital forensics capabilities in Nigerian Banks can be achieved through several potential solutions. Technological solutions: Implementing Artificial Intelligence (AI) powered tools can automate complex tasks, identify patterns, and analyse large datasets, improving the speed and accuracy of digital forensic investigations. Utilising machine learning algorithms can help detect anomalies and predict potential cyber threats, enabling proactive measures to prevent incidents. Capacity building and training: Specialised digital forensic training for digital forensic experts can enhance their skills and knowledge and enable them to handle complex investigations. Conducting a cybersecurity awareness campaign can educate individuals and staff about common cyber threats and safe online practices. Collaborating and partnering with Forensic Institutes and other cybersecurity bodies will help to facilitate knowledge sharing. Regulatory Framework: Establishing clear regulatory frameworks can ensure that digital forensic investigations are conducted with legal standards, ensuring the admissibility of the evidence in court. Engaging in international collaborations can enable the sharing of intelligence, best practices, and global expertise in cybersecurity and digital forensics. Investing in Cybersecurity: Investing in robust cybersecurity frameworks, including incident response plans and intrusion detection systems, can help prevent and respond to cyber incidents.

To explore the usefulness of digital forensics in criminal investigations in Nigerian Banks: Digital forensics is useful in criminal investigations in Nigerian banks, offering several benefits. Enhanced evidence collection: Digital forensics enables the collection and analysis of digital evidence, such as system logs, which can be important in investigating financial crimes. Improved Investigation Efficiency: Digital forensic tools and techniques can help investigators quickly identify and analyse relevant evidence, reducing the time and resources required for investigation. Increased Accuracy: Digital forensics can provide accurate and reliable evidence, which can help investigators build strong cases and increase the chances of successful prosecutions. Deterrent Effect: The use of digital forensics can deter potential cyber criminals from committing financial crimes, as they know that their activities can be tracked and analysed.

To achieve the stated objectives, research design was a sample survey while the population consists of staff of relevant departments like Internal Control (IT Control), E-Business & Operations Control, IT Audit, Electronic

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Fraud, Security Operation Centre, Cyber Security Fraud & Investigations of top five (5) banks in Nigeria Access Bank, United Bank for Africa (UBA), First Bank, Guaranty Trust Bank and Zenith Bank. The sample size was 150 selected in the sample survey. Structured questionnaires were used to get the data, while data were analysed using frequency tables, percentages and the hypotheses were tested using chi-square. **Conclusions** Digital forensics is now an exciting profession that places emphasis on the human element due to the need of uncovering digital evidence in an ever-changing digital ecosystem within the banking industry. The prospects of digital forensics in an ever-changing digital ecosystem is high considering that banking transactions has now moved from the branch offices of the banks to the digital changes (self-service channels) creating an exciting motivation for the customers as well as the cyber criminals. The banks are in the custody of two key motivators for cyber criminals – data and money and in effect has become too attractive to cyber criminals. The prospects of digital forensics in Nigerian banking industry includes:

Despite the enormous prospects of digital forensics in Nigerian banking industry, there are numerous challenges facing the profession with the banking industry in Nigeria and they include the following:

1. Limited Digital Forensic Resource: Nigeria's major financial crime investigation agencies, such as the Nigerian Police Force and Economic and Financial Crimes Commission (EFCC) lack sufficient digital forensic resources.
2. Inadequate Access to Advanced Digital Tools: Forensic experts in developing economies like Nigeria and, by extension, the Banking industry face restricted access to advanced digital tools, hindering their effectiveness in detecting and preventing financial crimes.
3. Shortage of skilled digital forensic professionals: The Nigerian Banking sector faces a significant shortage of skilled digital forensic experts, posing a major challenge to effectively combating cyber threats.
4. Insufficient investment in Digital forensics: Nigeria's cybersecurity investment is limited, with an estimated funding gap of $22B for African cybersecurity, making businesses and institutions like the banking industry vulnerable to cyber threats.
5. Lack of Awareness and Training: Many Nigerians and, by extension, bank staff lack awareness about common cyber threats and safe online practices, increasing the risk of cyber incidents.
6. Regulatory challenges: The banking sector faces unique cybersecurity challenges that necessitate a nuanced understanding and strategic approach, with the regulatory framework playing a crucial role in enhancing cybersecurity measures.

Acceptance and incorporation of digital forensics in nominal criminal investigation within the Bank will aid accuracy and speed in nailing or exonerating the defendants, especially now that most banking transactions are digitalised.

Recommendations

From the findings, the following solutions and recommendations are made:

1. Technical Solutions: Advanced training: Provide digital forensic experts with regular training on the latest technologies, tools, and techniques to stay ahead of emerging threats.

Specialised tools: Utilise specialised software and hardware tools, such as Encase, FTK, and X-ray Forensics, to analyse and extract data from digital devices and networks. Encryption solutions: Develop and implement effective decryption tools and techniques to access encrypted data.

2. Regulatory Framework: National Law: Establish a specific national law applicable to digital forensic investigations, ensuring standardisation and clarity. Regulatory Compliance: Ensure compliance with data protection regulations, such as the Nigeria Data Protection Regulation (NDPR). International collaboration: Engage in international collaborations to share intelligence, adopt best practices, and benefit from global expertise in cybersecurity.
3. Capacity Building: Education and Training: Invest in education and training programs to develop a skilled cybersecurity workforce, including specialised courses in digital forensics. Public Awareness: Conduct public awareness campaigns to educate individuals about cyber threats and safe online practices. Public-Private Partnership: Foster a partnership between the public and private sectors to enhance cybersecurity capabilities and facilitate knowledge sharing.
4. Investment in Cybersecurity: Cybersecurity Levy: Implement a cybersecurity levy to generate funds for cybersecurity initiatives. Investment in Infrastructure: Invest in robust cybersecurity frameworks, including incident response plans, intrusion detection systems (IDS), and encryption techniques.
5. Incident Response and Investigation: Digital Forensic Capabilities: Develop robust digital forensic capabilities to investigate cyber incidents, identify perpetrators, and understand attack vectors. Evidence Collection: Implement effective evidence collection and preservation methods to ensure admissibility in court.

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Incident Response Plans: Establish incident response plans to minimise damage, restore systems, and prevent future attacks.

REFERENCES

1. Casey, B. J., Thomas, K. M., Davidson, M. C., Kunz, K., & Franzen, P. L. (2002). Dissociating striatal and hippocampal function developmentally with a stimulus-response compatibility task. *Journal of Neuroscience, 22*, 8647 – 8652.
2. Casey, B. J.(2011). Behavioral and neural correlates of delay of gratification 40 years later. *Proceedings of the National Academy of Sciences, 108*(36), 14998–15003.
3. Craiger, P. (2008). Training and education in digital evidence. In Handbook of Digital and Multimedia Forensic Evidence (pp. 3–15). Springer. https://doi.org/10.1007/978-1-59745577-0_2
4. Crime prevention through environmental design - Wikipedia Retrieved December 26, 2016, from
5. Crime prevention through environmental design. CPTED watch. Retrieved December 26, 2016, from http://www.cpted-watch.com/
6. Datamining. (2012). *Journal of Information Security, 3*, 196–201.
7. https://doi.org/10.4236/jis.2012.33024
8. Fulbright & Jaworski L.L.P. (2006). Fulbright's 6th Annual Litigation Trends Survey Report.
9. Retrieved from
10. https://www.uscourts.gov/sites/default/files/fulbrights_6th_annual_litigation_trend s_survey_report.pdf
11. Kessler, G. C. & Haggerty, D. (2008). Pedagogy and Overview of a Graduate Program in Digital Investigation Management. *In Proceedings of the 41st Annual Hawaii International Conference on System Sciences* (HICSS-41). IEEE.
12. Meshram, B. B. & Sindhu, K. K. (2012). Digital Forensics and Cyber Crime Data-Mining. *Journal of Information Security, 3*, 196-201. https://doi.org/10.4236/jis.2012.33024
13. Nance, D. A., Hay, B., & Bishop, M. (2009). Digital forensics: Defining a research agenda.
14. Proceedings of the 2009 Digital Forensics Research Workshop.
15. https://www.researchgate.net/publication/221180538_Digital_Forensics_Defining_a_Res earch_Agenda
16. Saferstein, R. (2009). Forensic science: From the crime scene to the crime lab (4th ed.). Pearson Prentice Hall.
17. Schatz, B. (2007). BodySnatcher: Towards Reliable Volatile Memory Acquisition by Software. *In Proceedings of the 7th Annual Digital Forensics Research Workshop* (DFRWS 2007). Digital Investigation, 4(1), 126–134. https://doi.org/10.1016/j.diin.2007.06.011
18. Sindhu, K. K., & Meshram, B. B. (2012). Digital Forensics and Cyber Crime Data-Mining. *Journal of Information Security, 3*(3), 196–201. https://doi.org/10.4236/jis.2012.33024

Copyright © 2025 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.